CASE STUDY

CS-2026-10

ioSENTRIX

Your Trusted Partner in Cybersecurity



FINANCIAL SERVICES APPLICATION SECURITY

Four High-severity flaws found and fixed before a finance portal launched

Card numbers in HTTP responses and a referral feature open to phishing, closed before customers arrived.

CLIENT
Financial services company

SERVICE
Web application penetration testing

FOCUS
Card data and business logic

VERIFIED
Critical and High fixed; retested by ioSENTRIX

AT A GLANCE

CLIENT
Financial services company

PRODUCT
Multi-user web portal where corporate customers manage their finances

SERVICE
Web application and API penetration testing

SCOPE
The web application and the servers that handle and store customer data

DRIVER
An outside view of an application built in-house

VERIFIED
Critical and High fixed; retested by ioSENTRIX

TESTED BY
ioSENTRIX application security testers

EXECUTIVE SUMMARY

Card data in responses and phishing through the portal itself, both fixed before launch

A financial services company built a multi-user web portal for its corporate customers to manage their finances. Because the team had built it in-house, it wanted an outside view before launch.

Our testers found more than 25 issues, four of them High. Credit card numbers were exposed in HTTP responses, and the portal's referral feature could be turned into a phishing tool. The in-house team fixed every High finding before launch, and ioSENTRIX retested the fixes.

25+	4	1
findings across the portal and its servers	High-severity findings, all fixed before launch	referral feature that could send phishing from a trusted sender

The most dangerous feature was the one built to bring in new customers.

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

© 2026 ioSENTRIX LLC

01 What we found

HIGH FINDING 1

Card numbers came back in HTTP responses

Credit card numbers were included in the portal's HTTP responses, where anyone with access to the browser or the traffic could read them, whatever the page itself displayed.

Business impact: payment card data that should never leave the server in readable form was exposed.

HIGH FINDING 2

The referral feature could carry an attacker's phishing

Users could change the referral message without restriction. A message sent through the portal's own referral feature could carry an attacker's text and links.

Business impact: phishing would arrive from a trusted, legitimate sender, the portal itself, aimed at the company's own prospects.

Figure 1. Two High-severity paths found before launch



HOW WE FOUND IT

Our testers mapped every page and parameter, then used each feature the way both a customer and an attacker would, including the referral flow built to bring in new customers.

© 2026 ioSENTRIX LLC

02 Results

Figure 2. Findings by severity (25+ findings)



Figure 3. What changed before launch — **All High findings fixed before launch; retested by ioSENTRIX**

AREA	BEFORE THE TEST	AFTER REMEDIATION
Card data	Credit card numbers exposed in HTTP responses	● Exposure removed; fix retested by ioSENTRIX
Referral messages	Message text could be changed without restriction	● Fixed by the in-house team; retested by ioSENTRIX
Requests and workflows	Cross-site request forgery and a business-logic flaw	● Both fixed and retested before launch

03 Lessons for financial services teams

Never send what the page should not show

Card numbers in a response are exposed even if the screen hides them. Mask or drop sensitive data on the server.

Finding 1

Treat user-editable content as a channel

A referral message anyone can rewrite is a phishing tool with your name on it. Restrict what users can change.

Finding 2

Test features as an attacker would use them

The referral flow was built for growth. Testing it as an abuse path found the risk before customers did.

Approach · OWASP Web Security Testing Guide, 4.10 Business Logic

ioSENTRIX

Launching a financial application? See a sample web application test report or book a strategy session before go-live.

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.