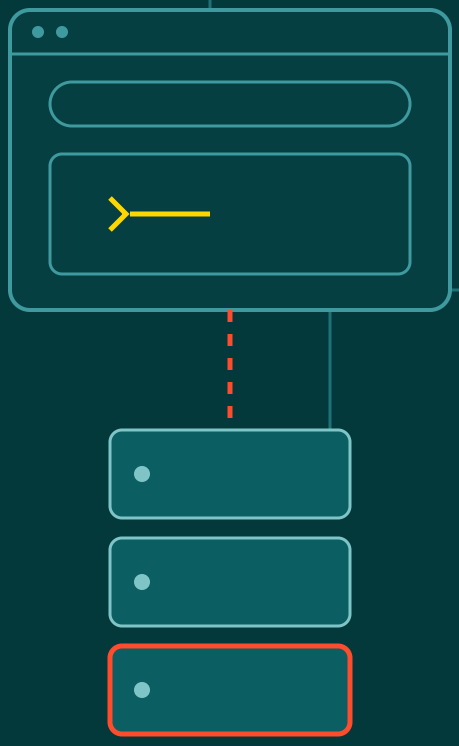
CASE STUDY

CS-2026-08

ioSENTRIX

Your Trusted Partner in Cybersecurity



FULL-STACK PENETRATION TESTING

How a locked-down kiosk browser led to domain administrator access

A pre-launch, full-stack test of a sensitive web application and its virtual desktop.

CLIENT
Professional services firm

SERVICE
Full-stack penetration testing

FINDINGS
10+, including 3 Critical

VERIFIED
Critical and High fixed; retested by ioSENTRIX

AT A GLANCE

CLIENT
Professional services firm

PRODUCT
Internal web application for sensitive client cases

SERVICE
Penetration testing

SCOPE
Web application, its virtual desktop (Citrix) environment and the network behind it

ACCESS
Black-box, kiosk-mode browser only

ENGAGEMENT
A multi-week engagement before launch

VERIFIED
Critical and High fixed; retested by ioSENTRIX

TESTED BY
ioSENTRIX application and network testers

EXECUTIVE SUMMARY

A kiosk-only start, a full compromise of the network, and gaps in the application itself

A professional services firm was about to launch an internal web application that manages its clients' sensitive cases. Users could reach it only through a virtual desktop that showed nothing but a kiosk-mode browser, watched by a security operations centre.

Our testers broke out of the kiosk, mapped the internal network and escalated privileges to administrator on the domain controller. In the application, they found cross-site scripting and missing authorisation checks. The client remediated the findings before launch, and ioSENTRIX retested the fixes.

1	10+	3
kiosk browser as the only way in	findings, 3 of them Critical	layers tested: application, virtual desktop and network

One escape from a kiosk window led all the way to the domain controller.

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

© 2026 ioSENTRIX LLC

01 What we found

THEME · INFRASTRUCTURE FINDING 1

A locked-down kiosk led to domain administrator

Our testers broke through the restrictions of the virtual desktop and launched built-in tools such as Explorer and Notepad. That opened the way to internal reconnaissance, which turned up several internally hosted applications, and then to privilege escalation and administrator access to the domain controller.

Business impact: a user limited to one browser window could have taken control of the whole network.

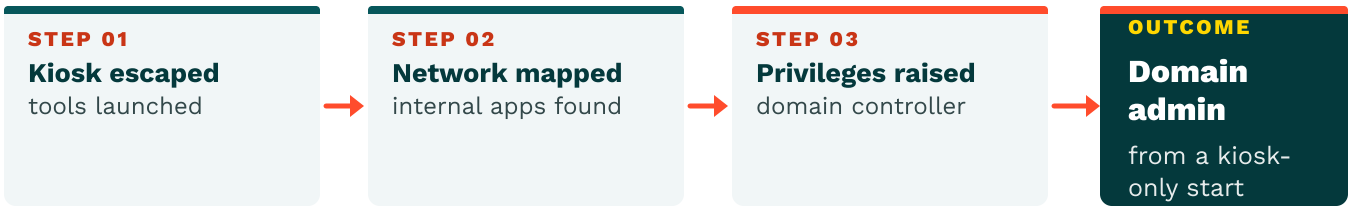
THEME · WEB APPLICATION FINDING 2

The application skipped checks it needed

The web application itself had cross-site scripting and missing authorisation checks of the kind needed to protect critical data.

Business impact: sensitive client case data could have been exposed or changed by users who should not see it.

Figure 1. One chain from a kiosk-mode browser to the domain controller



HOW WE FOUND IT Testing started from the same kiosk window a real user sees, then treated the browser, the virtual desktop and the network as one target, the way a compromised user would.

© 2026 ioSENTRIX LLC

02 Results

Figure 2. Findings by severity (10+ findings)



Figure 3. What changed before launch — **Critical and High fixed before launch; retested by ioSENTRIX**

AREA	BEFORE THE TEST	AFTER REMEDIATION
Domain control	A kiosk user could escalate to administrator on the domain controller	● Critical issues, including the privilege escalation, mitigated
Application	Cross-site scripting and missing authorisation checks on sensitive data	● Fixed by the client's staff, prioritised by severity
Launch	A sensitive application about to go live with unknown risk	● Launched with the findings addressed; fixes retested by ioSENTRIX

03 Lessons for launch teams

Kiosk mode is not a boundary

A locked-down browser was one breakout from the desktop. Treat the virtual desktop as part of the attack surface, not as its edge.

Finding 1

Test the whole stack together

The app, its virtual desktop and its network failed as one chain. Testing any layer alone would have missed the route to the domain.

Approach

Authorise every request

Missing authorisation checks exposed sensitive data. Being inside the network is not permission to see a record.

Finding 2 · OWASP Top 10 (2021) A01: Broken Access Control

ioSENTRIX

Launching a sensitive application? See a sample full-stack 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.