



CASE STUDY

From a web foothold to the entire data tier

Financial-data processor (multi-bank) · Internal / container-escape pentest

Full compromise chain, 24h P0 plan

Anonymised under NDA. Client and identifying details are withheld. PXL Security LTD · Sofia, Bulgaria · pxlsec.com

CASE STUDY

From a web foothold to the entire data tier

Sector	Financial-data processor (multi-bank)
Engagement	Internal / container-escape pentest
Outcome	Full compromise chain, 24h P0 plan

1	millions	0
container foothold	rows reachable across tenants	rows read or exfiltrated

THE CHALLENGE

A processor of regulated banking data for multiple tenant banks wanted to know the real blast radius available to an attacker who achieves code execution inside the production application container.

HOW IT UNFOLDED

1. Started from a simulated foothold inside one production app container.
2. Read decrypted secrets left in plaintext at container start.
3. Found the app's database account was a cluster superuser, reachable from the app.
4. Proved read/write across dozens of tenant databases, a central credit-risk dataset and the shared SSO store.
5. Recovered the production session-signing key — proven offline by reproducing a real signature — enabling forgery of any user, role or tenant.
6. Also recovered a GitOps deploy key and partner transfer keys (and their passphrases) from the same readable config.

KEY FINDINGS

Critical	Application DB account is a cluster superuser
Critical	Session-signing key recoverable from the app host
High	Decrypted secrets readable in the running container
High	GitOps deploy key exposed (supply-chain risk)
Medium	Partner transfer key passphrases stored alongside keys

IMPACT

A single container compromise escalated to cross-tenant data access, session forgery for any account, and a foothold back into the software supply chain.

OUTCOME

A fully-proven, step-by-step chain with a 24-hour P0 remediation plan: rotate the signing key, demote the database account, rotate deploy and partner keys. All capability was documented via metadata only — no customer rows were read.

TECHNIQUES

Secrets at runtime · Database superuser abuse · Session-key forgery · Supply-chain keys · Blast-radius mapping

SERVICES

Penetration Testing · Cloud Penetration Testing

Work with PXL Security

Independent offensive-security testing since 2014 — penetration testing, red teaming and secure development, delivered by senior engineers with evidence for every finding and a retest to prove the fix.

Request a proposal: pxlsec.com/contact · hello@pxlsec.com

PXL Security LTD · 12 Vasil Levski Blvd., 1142 Sofia, Bulgaria · VAT BG203239331