



CASE STUDY

Hardened, but not finished: a payment operations app

Retail bank — payment operations · Authenticated web app pentest

16 findings, SoD redesign path

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



CASE STUDY

Hardened, but not finished: a payment operations app

Sector	Retail bank — payment operations
Engagement	Authenticated web app pentest
Outcome	16 findings, SoD redesign path

16 findings	1 operator could reroute payments alone	0 injection/authz flaws
-----------------------	---	-----------------------------------

THE CHALLENGE

A bank asked for a gray-box test of a payment-operations web application from the perspective of its highest standard administrative role.

HOW IT UNFOLDED

1. Tested from the highest standard admin role (gray-box).
2. Confirmed the core controls — injection resistance, object authorization — were genuinely solid.
3. Found a routine profile field exported as a live spreadsheet formula, executing on whoever opened the export.
4. Found a role labelled benign “self-service profile” that actually granted full user and role administration.
5. Found high-impact payment-engine operations (date roll, resend, suspend, routing, start/stop) with no maker/checker approval.

KEY FINDINGS

High	No segregation of duties on high-impact payment operations
High	Misleading role label grants hidden full administration
Medium	Stored spreadsheet-formula injection in data export
Positive	Injection and object-authorization controls were sound

IMPACT

Strong technical defences were undercut by segregation-of-duties gaps that would let one insider — or one compromised operator — move or stop payments unilaterally.

OUTCOME

Sixteen findings centred on segregation of duties, role-label accuracy and safe data export, giving the bank a concrete path to second-actor approval and least-privilege role redesign in a high-value payment environment.

TECHNIQUES

Business logic · Segregation of duties · CSV/formula injection · Role-privilege mapping

SERVICES

Penetration Testing · Compliance-Driven Pen 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