



CASE STUDY

A shipped mobile app that was a credential vault

Enterprise SaaS / CRM · Mobile app pentest (Android, iOS, Windows)

1 Critical, 5 High — remediated

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

CASE STUDY

A shipped mobile app that was a credential vault

Sector	Enterprise SaaS / CRM
Engagement	Mobile app pentest (Android, iOS, Windows)
Outcome	1 Critical, 5 High — remediated

1C / 5H findings across 3 platforms	3 OS platforms tested	0 customer records exfiltrated
---	---------------------------------	--

THE CHALLENGE

An enterprise SaaS vendor needed its cross-platform hybrid CRM client — shipped to customers who hold live customer records — validated across Android, iOS and Windows.

HOW IT UNFOLDED

1. Treated the shipped app as an archive, not a program — unpacked and read the binary.
2. Found hardcoded backend credentials compiled into the bundle.
3. Confirmed (read-only) they granted a live, authenticated session to an internal customer-data API.
4. Recovered the at-rest database key from device-derivable material (weak, unsalted key derivation).
5. Decrypted the offline data store; bypassed jailbreak detection with a single runtime hook.
6. Showed an MDM default silently disabled TLS pinning — enabling full session interception.

KEY FINDINGS

Critical	Hardcoded backend credentials in the shipped binary
High	At-rest encryption key recoverable from the device
High	Embedded local runtime server leaks its own auth token
High	Certificate pinning silently disabled by an MDM default
Medium	Jailbreak/root detection bypassable with one hook

IMPACT

A motivated attacker with nothing but the public app could reach a live customer-data API and decrypt the offline store — on all three platforms.

OUTCOME

One Critical and five High issues with end-to-end runtime proof, a prioritised “rotate now” credential list, and concrete key-derivation, pinning and token-handling fixes. Testing stopped at proof — no customer records were exfiltrated.

TECHNIQUES

Binary reverse-engineering · Hardcoded secrets · Weak key derivation · Jailbreak/root bypass · TLS pinning bypass

SERVICES

Penetration Testing · Secure Development

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