



CASE STUDY

A clean bill of health — and the proof to back it

Transport & logistics · External network pentest (black-box, ~80 hosts)

0 exploitable Critical/High — assurance delivered

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

CASE STUDY

A clean bill of health — and the proof to back it

Sector	Transport & logistics
Engagement	External network pentest (black-box, ~80 hosts)
Outcome	0 exploitable Critical/High — assurance delivered

~80 public hosts tested	0 exploitable Critical/High	7+ headline CVEs proven non-exploitable
-----------------------------------	---------------------------------------	---

THE CHALLENGE

A logistics firm wanted a large internet-facing estate validated against current high-impact CVEs — reporting only vulnerabilities with a demonstrated, exploitable vector, not version-banner noise.

HOW IT UNFOLDED

1. Enumerated and fingerprinted roughly eighty public hosts across the testing window.
2. Actively tested each high-severity candidate CVE (mail-server RCE, edge-gateway memory-leak classes, device and portal CVEs, default-credential and service exposures).
3. Verified each was patched or non-exploitable — the edge gateway leaked no memory, the RCE vector wasn't reachable, reflected input was blocked by content-type and CSP.
4. Confirmed the few real, demonstrable issues: an exposed trace handler, anonymous FTP to an empty share, and missing SPF/DMARC.
5. Flagged one network block that was app-layer filtered to the tester's source and needs an allow-listed vantage to re-cover.

KEY FINDINGS

Medium	Exposed ASP.NET trace handler leaking request/session data
Low	Anonymous FTP accepted (empty share)
Low	No SPF/DMARC — email/domain spoofing possible
Positive	All headline CVEs proven patched / non-exploitable

IMPACT

The perimeter was materially hardened; residual risk was limited to information disclosure and email spoofing.

OUTCOME

High assurance that the headline CVEs were genuinely patched — proven, not assumed — plus a short, exploit-validated fix list and a retest plan for the filtered block. We report the good news too, with evidence.

TECHNIQUES

Exploit-only reporting · CVE validation · Attack-surface mapping · Email spoofing (SPF/DMARC)

SERVICES

Penetration Testing · Vulnerability Assessment

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