PENETRATION TEST · EXECUTIVE SUMMARY

Executive Summary

A four-minute read for the people who don't need the reproduction steps.

CLIENT	Pavex Commerce, Inc.
ENGAGEMENT ID	OW-2026-Q2-07
WINDOW	12 May – 02 Jun 2026
PREPARED FOR	CISO, audit committee, board of directors
COMPANION DOC	omegawulf-sample-report.pdf (10 pp.)
REPORT VERSION	1.0 — Final

CONFIDENTIALITY

This summary describes the results of an authorised security engagement performed for the named client. Detailed exploitation techniques and reproduction steps are intentionally excluded — they are covered in the companion technical report. Distribution is limited to the named recipient and their designated officers.

PAGE 02 · AT A GLANCE

Two critical findings. Both close this week.

Across three weeks of testing against your web application, public API, and AWS production estate, we identified seven findings of note. The two Critical issues are reachable from the internet and remediable inside one engineering sprint. The three High-severity issues concern customer-data exposure and pipeline-to-account privilege escalation in AWS. None of the issues required novel research; all were reproduced from known techniques.

CRITICAL	HIGH	MEDIUM	LOW	INFO
2	3	2	0	0
FINDINGS	FINDINGS	FINDINGS	FINDINGS	FINDINGS

POSTURE

Your perimeter is well-instrumented but exhibits two classes of drift that warrant immediate action.

PAGE 03 · WHAT AN ATTACKER COULD DO

Three things, and what they'd mean.

Stated in business terms. Technical reproduction is in the companion report.

01 Pose as your brand.

A motivated attacker could claim an abandoned marketing-tenant subdomain and stand up a credential-harvesting page under your real domain. Customers, merchants, and partners would see a page that is technically yours — same TLS, same parent domain — and behave accordingly. Brand and trust impact would land before any technical detection fired.

02 Take over any account from a stale link.

Password-reset links remain valid for 30 days and are not invalidated after use. An attacker who recovers a single old reset email — from a leaked email backup, a support transcript, browser history on a shared device, or a phished victim — could take over the account without further interaction. Administrator accounts are not exempt.

03 Walk from CI into the cloud account.

An attacker who compromises a single CI runner could escalate to administrator control of the production AWS account through a misconfigured deployment role. Detection coverage during this path is limited. The remediation is scope-tightening, not a re-architecture.

PAGE 04 · REMEDIATION OUTLOOK

Close in this order.

Sequenced for risk reduction per engineering-hour.

THIS WEEK

4 engineering hours · closes both Critical findings

- Reclaim the abandoned marketing subdomain and add the DNS check to CI.
- Lock the API token verifier to a single signing algorithm; rotate keys.
- Block public access on the production AWS account and revoke the legacy bucket policy.

THIS SPRINT

2–3 engineering weeks · closes all remaining High findings

- Tenant-scope order lookups at the data layer, not the controller.
- Constrain the deployment role's permission to delegate, with monitoring.
- Disable GraphQL introspection in production and add depth limits.

THIS QUARTER

Proactive hardening · pays for itself by the next engagement

- Audit cross-account snapshot sharing and add a continuous Config check.
- Add an organisation-level policy denying privilege delegation for sensitive roles.
- Adopt continuous AWS monitoring (see page 05).

PAGE 05 · NEXT STEPS

What happens next.

Debrief call

Scheduled 09 Jun 2026, 10:00 PT. Pack lead and the operators who ran the engagement attend. Plan to walk the technical report and answer questions from your engineering leads.

Re-test of closed findings

Each finding is re-tested before the engagement window closes, at no additional charge. We confirm closure or document the residual risk.

Continuous AWS coverage (optional)

OmegaWulf SCOUT — our AWS reconnaissance agent that found three of the seven issues in this report — remains attached to your estate for 30 days post-engagement at no cost. After that, continuous coverage is available as a standalone subscription.

ENGAGEMENT SIGN-OFF

ENGAGEMENT	OW-2026-Q2-07	PACK LEAD	M. Andersen · Pack 02
CLIENT	Pavex Commerce, Inc.	OPERATORS	6 · web, API, cloud
WINDOW	12 May – 02 Jun 2026	CONTACT	engagements@omegawulf.com