

QODY Demo — MASTER Bug Registar (pun cross-role UAT 2026-07-08)

QODY DEMO — MASTER BUG REGISTAR (kompletan cross- role UAT, 2026-07-08/09)

8 agenata (4 happy-path po ulozima + 4 kombinatorne matrice). 7/8 gotovo; kitchen KDS pending (blokirano reset-pw bugom — sam po sebi nalaz). Evidence po agentu u `~/system/evidence/uat-full/{owner,guest,superadmin,matrix-A-perms,matrix-B-state,matrix-C-payment,matrix-D-edge}/`.

? CRITICAL / BLOKERI (5)

C1 — Cross-ORG data leak (#105076) [backend, sec] — POTVRĐEN LIVE iz 2 ugla (matrix-A + owner). GET `/admin/venues` + `/admin/venues/{id}` vraćaju SVE venue-ove SVIH organizacija bilo kojoj autentifikovanoj sesiji (bilo koja uloga, nema role/tenant check). Leak: fee, branding, slug cross-org. Root: AdminRoutes.kt:74-99 (fix pattern već na PUT 101-118). NAJVIŠI prioritet.

C2 — Reset-password modal PRAZAN [frontend] — owner + kitchen UAT. POST `/admin/staff/{id}/reset-password` vraća 200 s temporaryPassword, ali UI modal display div prazan, "Kopiraj" kopira ništa. Owner nema način dobiti novi pw. (Ranija "PASS" verifikacija gledala network 200, ne UI prikaz — lekcija.) Blokirao i kitchen UAT.

C3 — Monri plaćanje mrtvo [external/config] — guest UAT. Monri injected iframe.js pravi malformed URL `"ipgtest.monri.com:/v2/"` (kolon bez porta) → iframe se ne učitava → guest ne može platiti, checkout dead-end. Naš kod (lightbox.js src) ispravan. Treba istražiti Monri merchant config/authenticity token (možda loš base URL u Monri postavkama).

C4 — Add-to-cart prekriven AI-chat FAB-om [frontend] — guest UAT (mobile). "DODAJ" dugme fizički ispod "Pitajte nas" FAB-a → tap otvara chat umjesto dodavanja. Blokira naručivanje na telefonu. Fix: z-index/pozicija.

C5 — SUSPEND je lažan [backend] — matrix-B. suspend samo set deleted_at, NE provisioning_state (koji gate provjerava). Suspendovan venue: owner postojeća sesija radi (200), GUEST NASTAVLJA naručivati (GuestRoutes bez provjere). SUSPENDED+PENDING_PAYMENT stanja dokumentovana ali nikad build-ana.

? MAJOR (3)

M1 — Suspend/activate bez potvrde [frontend/superadmin] — misklik mijenja live status merchanta, nema "jesi siguran", nema undo. **M2 — Audit log ne bilježi activate/suspend** [backend] — status se tiho flipne bez traga (kombinovano s M1 = opasno). **M3 — Raw error poruke korisniku** [frontend/backend] — (a) dupli slug → raw PSQLError 500 u UI (leak DB constraint, izgleda kao crash); (b) super-admin wrong-pw → raw JSON "401:{...}" u banneru; (c) merchant wrong-pw → netačno "session expired". Login banner postoji (Vizu fix) ali sadržaj sirov.

? MEDIUM (5)

- MED1 — raw i18n/feature-flag keys leak u UI: MENU.MODIFIERS, BRAND.WHITELABEL ("brand.whitelabel: ukljuceno"), REPORTS.ADVANCED (shared component bug)
- MED2 — Monri pay dugme hardcoded EN (data-language="en"), ignoriše locale
- MED3 — nema dup-table-label check (2 stola isto ime, različit QR = floor confusion)
- MED4 — nema max-length org/venue name (500 char overflow u review + listi)
- MED5 — /guest/splitbill 403 + /guest/payment/intent 404 na svaki guest load (leftover Stripe-era + feature-flag)

? LOW (7)

- merchant tabela overflow 6236px @1440 (Akcije off-screen) · nema edit menu-itema · AI describe 404×18 · Stripe Connect ne lokalizuje + stale "2%" fee · dashboard quick-actions ne prevode (HR/SR) · pretplate venue-ID identični truncated · search bez empty-state · invite venueSlug ne validiran vs token (ne bypass)

? ISTO / RADI (verifikovano)

Gate PENDING→ACTIVE airtight (12 ruta 403, cash-only ACTIVE radi); XSS escaped svuda; price/email/empty validacija; JWT verify + brute-force logout; superadmin rute odbijaju owner (403); menu CRUD; QR gen/regen; operating hours; tips; CSV export; 4-jezik switch (osim navedenih); logout/session invalidation; modal focus-trap/ESC.

HOUSEKEEPING

~15 leftover UAT test orgova + XSS-probe org u demo listi → cleanup (#105068).

BATCH FIX PLAN (nakon konsolidacije ? jedan merge ? jedan deploy ? re- UAT)

- **CodeCraft backend:** C1 (tenant-scope 2 GET), C5 (suspend→provisioning_state + GuestRoutes block + session revoke), M2 (audit activate/suspend), M3a (dup-slug friendly error), MED5 (guest 403/404), reset-pw response već radi (C2 je FE)
- **Vizu frontend:** C2 (reset-pw modal display), C4 (add-to-cart z-index), M1 (confirm dialog suspend/activate), M3b/c (friendly login/error poruke), MED1 (i18n keys), MED2 (Monri locale), MED3/4 (validacije) + VEĆ SPREMNO: invite-display (7609855), login-tabovi (2c71867)
- **Istražiti:** C3 (Monri malformed iframe URL — merchant config/authenticity token)
- **Cleanup:** #105068 (leftover test data)

Revision #1

Created 2026-07-08 23:10:00 UTC by John

Updated 2026-07-08 23:10:00 UTC by John