[redacted] Backend Gray-box Penetration Testing

[redacted] • May 2026 • Prepared by: Molly

CONTENTS

EXECUTIVE SUMMARY

This report summarizes a local security assessment of the [redacted] [redacted] backend. The assessment focused on tenant isolation, role enforcement, object ownership checks, and state-changing API behavior across [redacted] administration, users, orders, invoices, contributions, medication stock, [redacted] inspections, messaging, assets, and reference-data management. Testing promoted only high-confidence findings with request/response evidence, database before/after checks, and negative controls. The workspace contains 37 accepted findings: 25 high severity and 12 medium severity. The dominant risk is systemic authorization failure: many endpoints authorize a client-supplied [redacted] id, selected-[redacted] header, or request body value, then mutate or read a different route-selected or id-selected resource.

TARGETED ASSETS

`http://127.0.0.1:3333`

- **Version:** [redacted] [redacted] backend, local commit [redacted]
- **Notes:** Local target from cloned [redacted] repo. The target manifest identifies this as [redacted]-local.

METHODOLOGY

`OWASP API Security` `Broken Object Level Authorization` `Broken Function Level Authorization` `Tenant Isolation Review` `Role-Based Access Control Review` `[redacted] Source Review` `Authenticated API Testing` `Local Fixture Validation` `Manual Exploitation` `Database State Verification`

The assessment used a gray-box workflow against a local [redacted] backend and seeded [redacted] fixture. Source review identified authorization boundaries, route handlers, validators, [redacted] checks, and model relationships. Dynamic validation used controlled authenticated accounts with different [redacted] memberships and roles, unauthenticated controls, forbidden-route controls, local database before/after queries, reversible fixture changes, and request/response captures. Findings were accepted only when a concrete privilege or tenant boundary was crossed and a negative control showed the same actor was not otherwise authorized for the target [redacted] or resource. Destructive proofs were performed on local fixture data and cleanup was recorded where applicable.

TOOLS UTILIZED

curl-based HTTP probes

jq

[redacted]-backed assessment ledger

[redacted] local fixture queries

[redacted] route, controller, validator, and [redacted] source review

Fake [redacted]/object-store request recorder

Custom shell validation scripts

VULNERABILITIES

Cross-tenant user update enables foreign account takeover

CVSS 9.3 CRITICAL

CWE-639 CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:N/SC:H/SI:H/SA:N

Description: The user administration flow authorizes `PATCH /users/:id` against a [redacted] id supplied in the request body, then loads and mutates the route-selected user id without proving that the target user belongs to the authorized [redacted]. A [redacted] 1 manager used this mismatch to update [redacted] 2-only user accounts, change their email addresses, add attacker-controlled [redacted] memberships, trigger password reset, complete reset, and log in as the foreign users. Related identity-linking behavior in `POST /[redacted]` can also merge attacker-supplied profile data into an existing cross-[redacted] user by matching email.

Impact: A tenant manager can take over accounts from another tenant and inherit the victim user's data access and roles. The same primitive corrupts shared identity records, changes reset destinations, and can forcibly attach foreign accounts to the attacker's [redacted].

Remediation: Never authorize user mutations from a body-supplied [redacted] alone. Load the route-selected user first, derive the target user's existing [redacted] memberships from trusted storage, and require the caller to have a user-management role in at least one of those target memberships before changing identity, email, password-reset state, or relations. Separate self-service profile edits from tenant membership administration. Add regression tests for foreign user ids, body/route [redacted] mismatches, email changes, reset-token flows, and existing-email [redacted] creation.

Self-service profile and [redacted] update paths allow membership and role escalation

CVSS 9.4 CRITICAL

CWE-269 CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:L/SC:H/SI:H/SA:L

Description: `PATCH /users/me` accepts a [redacted] array and created a new active membership in an arbitrary [redacted] for a basic [redacted] 1 [redacted]. After self-joining [redacted] 2, the same token could access [redacted] 2 medication prices and create a [redacted] 2 purchase order. Separately, `PUT /[redacted]/:id` allows a [redacted] to manage their own profile and then writes submitted role values to the same [redacted] row. A basic [redacted] changed their role to [redacted] and immediately accessed a [redacted]-only user listing route.

Impact: Any authenticated user can grant themselves access to other tenant organizations or elevate from a basic [redacted] to an administrative role in their current tenant. Routes that trust membership or role checks become reachable after the self-modification.

Remediation: Make self-service account updates incapable of creating, deleting, activating, or changing [redacted] memberships and roles. Only dedicated administrative endpoints should mutate tenant membership or role state, and those endpoints must authorize against the target [redacted] and target user from trusted database records. Filter role fields server-side, ignore client-submitted role arrays on self-update, and add tests proving that basic users cannot self-add [redacted]s or upgrade roles.

[redacted] administration routes are reachable by ordinary authenticated users

CVSS 8.5 HIGH

CWE-862 CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:H/VA:H/SC:N/SI:H/SA:H

Description: Multiple [redacted] administration endpoints are protected only by generic authentication or by checks that do not bind the caller to the target [redacted]. A basic [redacted] could create new [redacted]s, update [redacted] metadata, deactivate arbitrary [redacted]s, modify foreign settings such as welcome-email behavior and contribution year, and change arbitrary [redacted] role page-access records. Negative controls showed the same account was not a national administrator and received 403 on ordinary [redacted] administration listings.

Impact: Any logged-in user can disrupt tenant availability, alter organization configuration, change contribution years, provision unauthorized [redacted]s, assign [redacted]s, and change page-level role access for other organizations.

Remediation: Require explicit [redacted] authorization on every [redacted] administration action. The route-selected [redacted] must be loaded from the database and passed to policy code before any write. Reserve create, activation, global update, and page-access operations for national administrators unless a narrower business rule is documented. Add route-level tests for create, update, activation, settings, year-of-[redacted], and page-access using basic [redacted], tenant manager, foreign manager, and national administrator accounts.

Financial and order workflows allow cross-tenant mutation through unscoped ids

CVSS 8.5 HIGH

CWE-639 CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:H/VA:L/SC:L/SI:H/SA:L

Description: Order, invoice, contribution, medication price, and credit-note routes repeatedly authorize one trusted-looking value and then mutate another id-selected resource. Confirmed examples include spending foreign credit notes through `POST /credit-notes/use`, marking foreign invoices and purchase orders paid through `POST /invoices/:id/payment`, reassigning and zeroing foreign purchase orders through `PATCH /purchase-orders/:id`, creating local orders linked to foreign distribution points through `POST /purchase-orders`, importing medication and contribution orders against foreign distribution points, mutating another [redacted]'s contribution settings, and updating another [redacted]'s medication prices by row id.

Impact: Attackers can corrupt tenant billing, contribution dues, medication pricing, invoice state, purchase-order ownership, payment records, and credit balances. Financial records can show paid status, consumed credits, zero totals, or foreign distribution-point links that do not reflect legitimate tenant activity.

Remediation: Treat every submitted object id as untrusted. For each mutation, load the target order, invoice, credit note, contribution, medication price, distribution point, and line item through a query constrained by the authorized target [redacted] and, where relevant, the authorized [redacted] or user. Reject mixed-[redacted] requests before writing. Use transactions so side-effect failures cannot leave partially committed financial state. Add matrix tests for body/route id mismatch, foreign distribution point ids, foreign credit note ids, foreign invoice ids, and foreign medication price ids.

Medication stock and prescription flows can modify another [redacted]'s inventory

CVSS 8.5 HIGH

CWE-639 CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:H/VA:L/SC:L/SI:H/SA:L

Description: Inventory routes authorize against the request query or the debit side of a transfer, but do not consistently verify the [redacted] of all referenced stock, medication, and user ids. A [redacted] 1 stock manager created stock-medication records inside [redacted] 2 stocks, credited transfer movements into [redacted] 2 stocks, and created prescriptions in [redacted] 1 that debited [redacted] 2 stock medication ids. Stock creation also accepted foreign [redacted] users as local stock managers.

Impact: A manager in one tenant can fabricate, credit, debit, or reassign another tenant's medication inventory and stock audit trail. This undermines medication availability, prescription accuracy, stock balances, and operational accountability.

Remediation: Model inventory operations around trusted stock ownership. Every `stockId`, `stockMedicationId`, `medicationId`, `managerId`, debit id, and credit id must be loaded with a join back to the authorized [redacted] before mutation. Transfers should require both debit and credit stocks to be in allowed [redacted]s according to an explicit business rule. Prescription stock debits must be constrained to the prescription's [redacted]. Add regression tests for foreign stock ids, foreign manager ids, cross-[redacted] transfer destinations, and foreign stock-debit ids.

Sanitary inspection report routes allow cross-tenant create, edit, approval, and deletion

CVSS 8.5 HIGH

CWE-639 CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:H/VA:L/SC:L/SI:H/SA:L

Description: Sanitary inspection handlers use selected-[redacted] authorization or route wrappers that do not bind the route-selected report id to the authorized [redacted]. A [redacted] 1 [redacted] user could create imported [redacted] reports in [redacted] 2, edit [redacted] 2 imported report conclusions and [redacted] comments, approve [redacted] 2 reports, and delete unapproved [redacted] 2 reports while ordinary [redacted] 2 report listing was forbidden.

Impact: A [redacted] user can forge, falsify, approve, or destroy another tenant's [redacted] inspection history and regulated report state. This compromises audit metadata, inspection conclusions, professional comments, exports, and downstream [redacted] workflows.

Remediation: Load every [redacted] report by id and authorized [redacted] together before update, approval, or deletion. Creation/import must prove that the selected [redacted], creator, [redacted], and report target belong to the authorized [redacted]. Remove any wrapper that authorizes a header/body/query [redacted] independently from the route-selected report. Add tests for foreign report ids across import create, import update, approve, delete, list, and export paths.

Asset endpoints expose arbitrary object-store key write and delete

CVSS 8.5 HIGH

CWE-862 CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:H/VA:H/SC:L/SI:H/SA:H

Description: `POST /assets/upload/:prefix?key=<raw-key>` and `DELETE /assets?key=<raw-key>` accept raw object keys and are protected only by generic authentication. A basic [redacted] uploaded and deleted controlled keys under [redacted] 2 and [redacted] 3-style prefixes; the fake object-store recorder observed the corresponding PUT and DELETE requests. The unauthenticated control returned 401, showing that the missing boundary is object ownership and tenant authorization, not route exposure.

Impact: A low-privileged account can overwrite or delete private bucket objects if keys are known or predictable. This can affect invoices, membership cards, prescriptions, uploaded documents, logos, signatures, report attachments, or other application files stored under the same object namespace.

Remediation: Do not expose raw storage keys as an authenticated public write/delete API. Generate keys server-side from a resource-specific owner and [redacted] context, store object metadata in the database, and authorize all upload/delete actions against that metadata. Deletion should require ownership of the parent domain object, not possession of a key string. Add tests proving users cannot write or delete keys outside their authorized tenant prefix or without a parent record.

Tenant configuration and master-data routes are vulnerable to body, query, and route id mismatches

CVSS 8.5 HIGH

CWE-639 CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:H/VA:L/SC:L/SI:H/SA:L

Description: Several configuration and reference-data routes authorize one [redacted] value while mutating another resource selected by route id, query id, or request body id. Confirmed examples include overwriting and reassigning foreign distribution points, changing another [redacted]'s document and GDS document parameters via route/body mismatch, creating/updating/deleting foreign groups, deleting foreign sectors through body/query [redacted] split, adding and removing cities on foreign sectors, editing/reassigning/deleting foreign [redacted] for shared users, creating local [redacted] for users who only belong to another [redacted], and assigning foreign users as local stock managers.

Impact: Tenant managers can corrupt or steal another [redacted]'s operational configuration, geographic sectors, document branding, groups, distribution points, [redacted] inventory, and responsibility assignments. These records feed downstream order, invoice, PDF, [redacted], stock, and user-filtering workflows.

Remediation: Adopt a single ownership rule for every route: authorize the caller against the persisted owner of the resource being read or mutated, not against a parallel client-supplied [redacted]. Route ids, query ids, and body ids must be cross-checked after loading resources from the database. Validators can check shape, but controllers and policies must enforce ownership. Add generic helper queries or policy methods for `loadForGdsaOrFail` and use them consistently across distribution points, sectors, document parameters, groups, [redacted], and stock ownership.

Cross-tenant messaging and membership discovery expose privacy boundaries

CVSS 5.3 | MEDIUM

CWE-200 | CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:N/SC:L/SI:L/SA:N

Description: Privacy-scoped routes disclose or act on users outside the caller's authorized tenant scope. The [redacted] import verifier lacks authorization and returns `UNIQUE_EMAIL` validation errors that reveal whether target emails belong to another [redacted]. The message sender authorizes the source [redacted] but accepts arbitrary recipient user ids, creating recipient rows for foreign-only users. [redacted] sector restrictions are disabled for authenticated [redacted] listings because the restriction helper returns early when `auth.user` exists, allowing a sector-limited [redacted] to list out-of-sector [redacted].

Impact: Attackers can enumerate cross-[redacted] membership by email, send or trigger messages to users outside the authorized tenant, and bypass sector privacy restrictions. These weaknesses support phishing, spam, membership discovery, and unnecessary exposure of [redacted] records.

Remediation: Authorize import verification against the requested [redacted] before running uniqueness checks, and normalize validation responses where practical. For messaging, require every recipient to belong to the sender's authorized [redacted] or to an explicitly allowed relationship. Fix [redacted] restriction logic so authenticated users are still constrained by assigned sectors. Add tests for foreign emails, foreign recipient ids, and out-of-sector [redacted] listings.

Deactivated [redacted]s remain accessible to users who have another active membership

CVSS 5.3 | MEDIUM

CWE-863 | CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:N/SC:L/SI:L/SA:N

Description: Login blocks users only when all linked [redacted]s are inactive. After a multi-[redacted] user logs in through an active [redacted], downstream authorization checks do not consistently verify that the requested [redacted] itself is active. A multi-[redacted] account with active [redacted] 1 membership could access protected [redacted] 2 stock and [redacted] routes while [redacted] 2 was deactivated; an inactive-only [redacted] 2 user was correctly rejected at login.

Impact: Deactivation does not reliably suspend access to an organization. Users with another active membership can continue reading or using protected routes for a deactivated [redacted] according to their old roles, undermining suspension, offboarding, and incident-response controls.

Remediation: Enforce active-state checks at the same point as per-route [redacted] authorization. A route that targets `[redacted]=X` should require both an allowed user membership and `gdsas.is_active=true` for X, unless the route is explicitly an administrative reactivation path. Add regression tests for inactive-only users, multi-[redacted] users, deactivated target [redacted]s, and national-admin exceptions.

SYSTEMIC WEAKNESSES

Authorization design trusts client-selected tenant context

HIGH

CWE-863

Description: Across many controllers, authorization is performed against `body.[redacted]`, `query.[redacted]`, [redacted], or another caller-controlled value, while the actual target resource is selected later by route id or submitted object id. This creates a recurring class of body/route/query mismatch vulnerabilities rather than isolated endpoint mistakes.

Impact: Fixing individual endpoints without changing the pattern is likely to leave similar flaws in adjacent routes and future features.

Remediation: Centralize authorization around persisted resources. Route handlers should load the target resource with its owner [redacted], call a policy against that loaded resource, and then mutate only that resource inside a transaction. Add reusable helper APIs and tests that make mismatched route/body/query [redacted] values a standard negative case.

CONCLUSION

The [redacted] backend currently has a systemic tenant-authorization problem. The most urgent fixes are the foreign account takeover path, self-service membership and role escalation, and [redacted] administration routes reachable by ordinary users. Next, the same ownership model must be corrected across financial/order flows, medication inventory, [redacted] reports, assets, and tenant configuration routes. The remediation should not be a set of local patches that special-case each reproduced request. The robust fix is to make resource ownership explicit, authorize loaded resources rather than client-supplied tenant ids, reject mixed-[redacted] payloads consistently, and preserve the 37 accepted findings as regression tests.