LAV'S INDUSTRIES

CAUCE · SECURITY AUDIT

Executive summary

Case Management Platform

SAMPLE REPORT · NO CLIENT DATA

Client	Client (public sector)
Scope	Sample based on a real audit, generalized
Reference	«commit reference withheld»
Run	run-1 · profile standard
Date	2026-09-23
Document	AUD-01

Executive summary

3	5	8	1	2
CRITICAL	HIGH	MEDIUM	LOW	NEEDS VALIDATION

What needs attention first

3 critical findings let an account holding a single ordinary permission take full control of the application. They share one root cause: nothing in the system checks that whoever edits permissions is not granting themselves more than they already hold.

Where things stand

Authorization rests almost entirely on route middleware: there is a single policy class in the whole application. That concentrates the risk in two places.

First, no point where access-control data is modified enforces a privilege ceiling. **Second**, several routes were left without the middleware their sibling routes carry; since there is no other authorization layer, those routes have none at all.

On the positive side: input validation is solid, no SQL injection was found, the password-recovery flows resist enumeration, and URL signing and token expiry are correctly implemented. The weaknesses are structural and concentrated, not scattered.

Findings by severity

SEVERITY	FINDING	DEMONSTRATED EFFECT
CRITICAL	**Permission-assignment endpoint with no privilege-ceiling check** SAMPLE-14	The endpoint that syncs a role's permissions never compares what is being granted against what the person performing the operation already holds. An account with a single narrow permission —…
CRITICAL	**Role rename with no reserved-name list allows impersonating the highest-privilege role** SAMPLE-13	The application's global authorization recognizes the highest-privilege role by its name. Because the role-editing endpoint does not protect that name, a holder of an intermediate administra…
CRITICAL	**User create and edit accepts a role field without validating the resulting privilege** SAMPLE-18	The user create and edit operations accept a field that assigns the role directly. The role is validated to exist, but not that the caller is entitled to grant it. A holder of the ordinary u…
HIGH	**Attachments served inline with a content type inferred from the file** SAMPLE-03	Attachments are validated by extension, but the content type they are served with comes from sniffing the bytes at upload time, and they are delivered for rendering inside the browser. A fil…

SEVERITY	FINDING	DEMONSTRATED EFFECT
HIGH	**Case sub-resources do not inherit the access control of the case** SAMPLE-16	The parent case is correctly protected, but its sub-resources — comments, assignment history and attachments — were left with no permission check. An account denied access to the case can re…
HIGH	**National-identifier directory readable by any authenticated account** SAMPLE-06	The people-directory read routes were left with no permission check: being authenticated, with zero permissions assigned, is enough to list and search national identifiers and personal data …
HIGH	**Organization scoping is optional rather than enforced on lists and exports** SAMPLE-08	The organization filter exists as an optional query parameter, not as an enforced restriction. An operational account assigned to a single organization can list and export records belonging …
HIGH	**Permission rename allows colliding with names used in authorization decisions** SAMPLE-09	When authorization resolves by permission name, being able to rename a permission is equivalent to being able to grant it. A holder of the permission-editing permission can rename one they a…
MEDIUM	**A second reassignment route skips the closed-case lock** SAMPLE-11	The primary endpoint refuses to reassign a case that is already resolved or closed. The alternate route producing the same mutation does not apply that lock, allowing cases that should be fr…
MEDIUM	**A second reassignment route skips the organization restriction** SAMPLE-10	The primary reassignment endpoint verifies that a coordinating role cannot move cases outside its own organization. A second route produces exactly the same change and carries no such check.
MEDIUM	**Closing a case validates neither the prior state nor the assignment** SAMPLE-15	The close operation does not check what state the case is in, nor whether the caller is the assigned owner. Any staff account can close any case, repeatedly, producing duplicate entries that…
MEDIUM	**Data export has neither rate limiting nor a per-user cap** SAMPLE-01	Any operational account can queue exports with no restriction on frequency or concurrent jobs. Repeating the request saturates the processing queue and consumes server storage.
MEDIUM	**Internal notes are not filtered out of the staff-facing listing** SAMPLE-05	A flag distinguishes internal notes from communication visible to the requester. The public endpoint respects it; the internal one does not filter on it. On top of that, any account can set …
MEDIUM	**Restoring a deleted account reinstates its previous credentials** SAMPLE-02	The block operation revokes active access credentials; restoring a soft-deleted account does not. A token issued before deletion silently works again after restoration, within its validity w…
MEDIUM	**Sign-in reveals account state before verifying the password** SAMPLE-07	The response distinguishes between nonexistent account, wrong password, blocked account and lockout, without the caller proving they know the password. The route also has no rate limit, whic…

SEVERITY	FINDING	DEMONSTRATED EFFECT
MEDIUM	**The user directory is exposed to any authenticated account** SAMPLE-19	The user-lookup routes are the only ones in their group without a permission check. They expose the email, block state and role and permission assignment of every account, which makes pickin…
LOW	**Reassignment does not validate that the recipient is active and eligible** SAMPLE-12	Neither reassignment route checks that the destination account is active, unblocked, and holds a role able to handle cases. A case can end up assigned to a blocked or deleted account, where …
NEEDS VALIDATION	**Attachments stored in a location the web server may be exposing** SAMPLE-04	Files are written to a directory whose configuration is intended for public exposure. The download model uses signed, expiring links, but if the deployment enabled the symbolic link that pub…
NEEDS VALIDATION	**Request origin may not be trustworthy behind a proxy** SAMPLE-17	There is no configuration declaring which proxies are trusted. If the production environment sits behind an undocumented load balancer, CDN or reverse proxy, the source address recorded in t…

Order of attention

ORDER	WORK BLOCK	EFFORT
1	**Contain privilege escalation** These let an account with one ordinary permission take full control of the application.	1–2 days
2	**Close the unauthorized routes** Routes that were left without middleware; the fix is one line and the risk is high.	Hours
3	**Harden the case lifecycle** These affect workflow integrity and availability, not data exposure.	2–4 days
4	**Confirm the pending items with your infrastructure team** They depend on a deployment fact that is not in the code. Confirming them is quick.	1 hour

Limits of this exercise

This was a first pass over the repository, reviewing source. The environment had no interpreter available, so no application code was executed: every finding rests on reading the source, and the two pending items depend on deployment facts that no file in the repository can answer.

Coverage was deliberately closed after the fourth round. By then five instances of the same underlying pattern had surfaced across successive rounds, which makes it likely — not merely possible — that more instances exist that this pass did not reach. That is stated as residual risk rather than presenting the coverage as exhaustive.