SECURITY ASSESSMENT REPORT

# Ledgerly (lab, release acceptance run)

Results of the security assessment of 10.250.0.16/32, 10.250.0.17/32, rv-laravel-lab: findings ranked by severity, with evidence and remediation guidance.

CLIENT

Ledgerly (lab, release acceptance run)

ENGAGEMENT

bench-acceptance-laravel

TESTING PERIOD

2026-11-10 to 2026-11-10

REPORT DATE

2026-11-10

PREPARED BY

RiskVoid

VERSION / STATUS

1.0 · Final

C

SECURITY POSTURE

Moderate exposure: 1 open finding, highest medium.

01 · EXECUTIVE SUMMARY

# What we found

This bounded release-acceptance assessment reviewed Ledgerly Laravel 12 source and compared selected behaviors on vulnerable .16 and fixed .17 deployments. The vulnerable deployment matched the supplied source; the fixed deployment was assessed at runtime only. This is a focused acceptance exercise, not a comprehensive security certification.

Three issues were reproduced on the vulnerable build: one High finding for member-to-administrator profile mass assignment, and two Medium findings for cross-tenant invoice/document disclosure and search SQL injection. All are P1 priorities because they threaten tenant permissions or financial-data confidentiality. Duplicate authorization instances were grouped under one root cause.

The fixed build resisted the tested profile role escalation and boolean search payloads. Invoice owner reads succeeded while foreign reads were denied in both API directions and the tested web direction. The fixed foreign-document request returned 403; a successful owner-document download remains unsupported, so the combined authorization retest is partial. Bob's role was restored and separately verified as member on both builds. All cleanup items are complete; seeded account/session retention remains operator-managed.

Coverage has explicit outcomes, including blocked and excluded work. Limitations include unsupported owner downloads, wrong-auth-mode matrix cells, missing runtime route export and PHP Joern support, untested stored-output experiments and broader privilege fields, and bounded dependency/secrets checks. The operator must set client metadata, review these limitations and approve the report before delivery.

| CRITICAL | HIGH | TOTAL FINDINGS | POSTURE |
|---|---|---|---|
| 0 | 1 | 3 | C |
| confirmed | confirmed | 2 resolved | moderate exposure |

FINDINGS BY SEVERITY 3 TOTAL

1 high  2 medium

02 · FINDINGS REGISTER

# All findings

| ID | SEVERITY | FINDING | CWE | STATUS |
|---|---|---|---|---|
| F-002 | HIGH | Mass assignment privilege escalation via PATCH /api/profile ($request→all())<br>http://10.250.0.16:8000 (rv-laravel-lab) | CWE-915 | RESOLVED |
| F-001 | MEDIUM | Missing tenant authorization exposes invoices and documents<br>http://10.250.0.16:8000 (rv-laravel-lab) | CWE-862 | OPEN |
| F-003 | MEDIUM | Search SQL injection bypasses the tenant filter<br>http://10.250.0.16:8000/search?q= | CWE-89 | RESOLVED |

03 · SCOPE

# Scope and rules of engagement

Testing was limited to the targets below. The limits were enforced technically: every command ran in a per-engagement sandbox whose network access was restricted to these targets, at or below the agreed intensity, and every command was recorded in an audit log.

| TYPE | TARGET |
|---|---|
| Network | `10.250.0.16/32` |
| Network | `10.250.0.17/32` |
| Source code | `/src/rv-bench/rv-laravel-lab` |

| RULE | VALUE |
| --- | --- |
| Allowed testing tiers | PASSIVE ACTIVE INTRUSIVE |
| Maximum request rate | 10 per second |
| Network access | online |
| Testing window | unrestricted |
| Testing period | 2026-11-10 to 2026-11-10 |

04 · METHODOLOGY

# How we tested

Testing followed the source-assisted Laravel playbook with bounded adaptations of web-app, API-security, code-review, supply-chain and secrets-review checklists in PLAN.md. Scope: /src/rv-bench/rv-laravel-lab, 10.250.0.16:8000 and 10.250.0.17:8000. Policy revision 9124ff4962c8fba1; maximum rate 10/s. Only these lab hosts were tested.

Sequence: static Laravel map and build identity, PHP Semgrep (25 app files), working-tree Gitleaks, OSV composer.lock (112 packages), manual controller/policy/Blade/config review, baseline login/404/tooling/anonymous API requests, console-approved read authorization matrix, individual failure repeats, and approved bounded boolean SQL injection browser experiment. Matrix: 31 pass, 5 FAIL, 24 blocked; blocked cells are not safety results. Bearer accounts on web routes were labeled session-ended by the kit despite later valid identity checks; mode-aware matrices are recommended.

Approvals were host/console decisions. The first browser experiment reproduced vulnerable search SQL injection and fixed invoice denial, then exited with Download is starting at the fixed owner document. Foreign document and later fixed-search steps did not run. A changed continuation was separately proposed for approval. A preliminary script exited with a missing credential environment variable before login or injection; it is not a completed SQL test. No approval bypass or credential export was attempted.

Evidence consists of audited runs, HTTP exchanges, the map, matrix and browser summaries/requests with SHA-256 provenance; worker transcripts are not finding

evidence. OSV empty results required an explicit osv-scanner parser after auto-detection selected Semgrep: import I-005 is authoritative for that file. No persistent fixture changes or mail sends occurred; only ephemeral login sessions were created.

Vulnerable build: ec5377ef5b4e73f11814f27e8cc798d1791ef83238a4a8f18ac3664d9318de6a (source match). Fixed runtime build: aacce094b7bcbc6e81cd28913f480f7c461db35630649652c31bc0161eb429d8 (fixed source not supplied). No claims of a full ASVS/WSTG assessment or complete two-scanner supply-chain review are made. The separately approved fixed-search continuation (96753bd6) completed with exit 0: valid Acme dashboard and empty normal/true/false query results. Evidence: evidence/runs/20261110T153822-python-679d08.txt and evidence/browser/20261110T153820-76f27d/summary.json. The search experiment needed two approvals because the first run stopped on download; no additional vulnerability class was exploited.

## Approved completion and fixed-build retests

Following service recovery, separate console approvals authorised Bob's own role-only profile test and restore on each build: 1fac7878, 94f93f70, d0ca8e2d, be6336b2. Vulnerable .16 persisted admin; fixed .17 retained member. Separate final GET /api/me checks verified member on both builds (evidence/http/20261110T155152-get-10.250.0.16-f7abff.txt and evidence/http/20261110T155152-get-10.250.0.17-dbf174.txt). This supersedes earlier statements that profile testing was deferred or no persistent fixture change occurred: the temporary role change was restored; no invoice changes or mail sends occurred.

Approval 7695e45a authorised the fixed browser continuation. It established valid Acme login, successful owner invoice/search controls, foreign invoice 404, foreign document 403, and empty normal/true/false injection results. Evidence: evidence/runs/20261110T154909-python-46cff5.txt and evidence/browser/20261110T154907-a163bb/summary.json. Four additional fixed API reads verified tenant isolation in both directions. T-001 and T-002 record resolved fixed-control retests for profile and search; T-003 records partial authorization retest because successful owner-document download remains unsupported. Original .16 findings remain applicable; fixed status applies to the named .17 build only.

Each activity is classified by tier: **passive** (code and configuration analysis, research), **active** (scanning, crawling, fingerprinting) and **intrusive** (exploitation, brute force).

Intrusive commands require explicit, single-use approval. Automated tool output was triaged by a consultant: only findings confirmed against the evidence are reported.

31 commands were run (28 passive, 3 intrusive); 1 was refused by the policy engine; 7 intrusive actions were approved and 0 denied.

100 HTTP requests were sent one at a time through the audited request tool (96 active, 4 intrusive); 3 more were refused. 1 authorization matrix run compared what each test identity could reach with what it should be able to reach.

| TOOL | USED FOR | RUNS |
|---|---|---|
| `semgrep` | Static analysis of the source code | 1 |
| `gitleaks` | Secrets in the repository and its history | 1 |
| `osv-scanner` | Known vulnerabilities in dependencies | 1 |
| `rv-llm` | LLM, agent and MCP server testing: prompt injection probes with canaries, tool-call checks | 1 |
| `scripts (python, python3)` | Checks written for this engagement, run in the sandbox | 4 |
| `other` | Helper commands (file handling, set-up) around the tools above | 4 |

### Severity rating

Severity reflects the impact and likelihood of exploitation in this environment. For known vulnerabilities in third-party components, the CVSS base score is adjusted using CISA's Known Exploited Vulnerabilities catalogue and the FIRST EPSS probability of exploitation.

05 · COVERAGE

## Coverage and limitations

26 tests were planned for this scope from the testing playbooks; 17 were carried out, of

which 4 found an issue; 5 could not be run; 4 were excluded or did not apply.

| AREA | PLANNED | NO ISSUE | ISSUE FOUND | BLOCKED | EXCLUDED | NOT RUN |
|---|---|---|---|---|---|---|
| Orientation and build identity | 4 | 3 | 0 | 1 | 0 | 0 |
| Pattern analysis | 3 | 3 | 0 | 0 | 0 | 0 |
| Identities and fixtures | 2 | 2 | 0 | 0 | 0 | 0 |
| Authorization | 4 | 1 | 2 | 0 | 1 | 0 |
| Input handling | 4 | 1 | 2 | 1 | 0 | 0 |
| Configuration | 4 | 3 | 0 | 0 | 1 | 0 |
| Fixed comparison | 1 | 0 | 0 | 1 | 0 | 0 |
| Authorization limitations | 1 | 0 | 0 | 1 | 0 | 0 |
| Bounded acceptance exclusions | 1 | 0 | 0 | 0 | 1 | 0 |
| Source limitations | 1 | 0 | 0 | 0 | 1 | 0 |
| Unsupported tooling | 1 | 0 | 0 | 1 | 0 | 0 |

## Not tested, and why

The tests below did not produce a result that this report can rely on. A weakness in these areas would not have been found by this assessment.

| TEST | WHAT IT CHECKS | OUTCOME | REASON |
|---|---|---|---|
| P-004 | Routes: the map's static routes. If the user can provide php artisan route:list --json (from the client, | Blocked | Static routes mapped. Runtime export not supplied; unblocks with operator-generated isolated php artisan route:list --json. |
| P-016 | unescaped-output leads: who can write the field, and who sees it. Store a harmless marker | Blocked | Invoice notes reach unescaped Blade via validated string update; no stored markup/browser experiment performed. Needs approved fixture write/restore and fixed web identity. |
| P-022 | Fixed document download owner/foreign controls | Blocked | Updated: fixed authenticated foreign document 2 now tested and denied 403. Owner download success still unsupported in browser; full paired document control remains blocked, not a pass. |
| P-023 | Wrong-auth-mode matrix cells and missing Globex web/member fixtures | Blocked | 24 matrix cells blocked: wrong auth mode returns 401 labeled session ended; alice-web limited to .16; no Carol web/Globex member. Validity rechecks succeed. Needs web identities for corresponding hosts/roles and typed mode-aware matrix handling. |
| P-026 | PHP Joern data-flow frontend | Blocked | Kit has no working PHP Joern frontend/binary, confirmed by map. Use supported PHP data-flow tooling if additional assurance needed. |

| TEST | WHAT IT CHECKS | OUTCOME | REASON |
|---|---|---|---|
| P-012 | Function-level: admin-only routes as a member (can: middleware, policies' before, is_admin checks). Refs: WSTG-ATHZ-03, API5:2023, ASVS V8. | Excluded | Member/admin write authorization source-reviewed only; runtime PUT/send needs extra intrusive experiments beyond agreed one-check budget. |
| P-021 | External effects: mail, notifications and outbound HTTP the map lists. Don't trigger them on a deployment | Excluded | Invoice send triggers mail + status change. Source describes log mailer, but no send effects triggered; outside one read-only injection acceptance experiment. |
| P-024 | Generic web/API broad scans and stateful business/session tests | Excluded | Narrow acceptance budget: no brute force, rate/DoS, broad web/API fuzzing, mail, workflow/race, stateful logout/CSRF attacks, client-side audit. HTTP only; GraphQL/JWT/WordPress/AI absent in mapped app. |
| P-025 | Second dependency scanner, SBOM, CI and secrets-history checks | Excluded | One OSV scan and Gitleaks working-tree only; no second scanner/SBOM/CI/maintainer review within budget. Mounted source has no git history; history analysis unsupported. |

# Findings

F-002 HIGH · CWE-915 RESOLVED

## Mass assignment privilege escalation via PATCH /api/profile ($request->all())

http://10.250.0.16:8000 (rv-laravel-lab)

| SEVERITY | CVSS | CWE | STATUS |
| --- | --- | --- | --- |
| High | 8.1 | CWE-915 | Resolved |

### CVSS VECTOR

`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N`

### DESCRIPTION

The self-profile endpoint mass-assigns untrusted request fields. A valid Acme member (Bob, user 2) sent PATCH /api/profile with only {"role":"admin"} on vulnerable .16. The response and a separate GET /api/me both showed role=admin. The approved restore changed it back to member.

On fixed .17 the identical approved request returned role=member; a separate read confirmed it stayed member. The tested role-escalation allegation is rejected for the fixed build. Tenant reassignment, password changes and platform-admin escalation were not tested and are not claimed.

### IMPACT

A member can promote their own account to tenant administrator. The supplied InvoicePolicy permits administrators to update tenant invoices, putting financial-record integrity and tenant-admin access at risk. No invoice mutations or administrator actions were performed.

### STEPS TO REPRODUCE

- As bob-api, GET /api/me; verify user 2, role member, organization 1.
- With console approval, PATCH /api/profile with Content-Type application/json and body {"role":"admin"}.
- GET /api/me separately; on .16 role is admin; on .17 it remains member.

- With separate approval, PATCH {"role":"member"} and verify restoration.

REMEDIATION

Allow-list validated self-service fields (such as name and timezone) using a Form Request and update($request→validated()). Never accept role, organization_id or is_platform_admin from self-profile input. Protect privilege changes with separate administrator-authorized operations and regression tests.

EVIDENCE

| FILE | SHA-256 | INTEGRITY |
| --- | --- | --- |
| `evidence/runs/20261110T154550-cat-c9be74.txt` | e2340150da7c0ebb… | PASS |
| `evidence/runs/20261110T155125-cat-40f59e.txt` | 04aa239fa0479f9f… | PASS |
| `evidence/http/20261110T154549-get-10.250.0.16-831372.txt` | dd85062b686de9b0… | PASS |
| `evidence/http/20261110T154550-get-10.250.0.17-bb1fd1.txt` | 67ae8d07de9b0376… | PASS |
| `evidence/http/20261110T154841-patch-10.250.0.16-342247.txt` | 3b2b3d56b57933ac… | PASS |
| `evidence/http/20261110T154858-get-10.250.0.16-448337.txt` | ad13f79d49b9d694… | PASS |
| `evidence/http/20261110T154841-patch-10.250.0.17-fd7fe4.txt` | 5e4b9ea6eb463c92… | PASS |
| `evidence/http/20261110T154858-get-10.250.0.17-ddaa7f.txt` | 08b1f0b661740973… | PASS |
| `evidence/http/20261110T154907-patch-10.250.0.16-ac1250.txt` | 0b4d18042c809a9d… | PASS |
| `evidence/http/20261110T154907-patch-10.250.0.17-fc70a2.txt` | 1653762a6fe18c45… | PASS |

F-001 MEDIUM · CWE-862 OPEN

# Missing tenant authorization exposes invoices and documents

http://10.250.0.16:8000 (rv-laravel-lab)

| SEVERITY | CVSS | CWE | STATUS |
| --- | --- | --- | --- |
| Medium | 6.5 | CWE-862 | Open |

## CVSS VECTOR

`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N`

## DESCRIPTION

Authenticated users on vulnerable .16 can read another tenant's invoices through web/API routes and download its documents. Global object binding is followed by missing tenant policy checks. Alice received Globex invoice 3 and document 2 with confidential fixture markers; the approved matrix also reproduced reverse-direction API access as Carol. Anonymous requests were denied.

Fixed .17 retest: API owner reads succeed and foreign reads return 404 in both directions. Valid Acme web login permits invoice 1 and denies invoice 3 (404) and foreign document 2 (403). The tested foreign-read allegations are rejected for the fixed build. However, a successful fixed owner-document download is still unavailable due browser download limitations; the document retest remains partial, not a complete safety claim. Fixed source was not supplied.

## IMPACT

A legitimate customer account can disclose another customer's invoice amounts, customer details, confidential notes and contract contents. Integrity/availability effects were not tested.

## STEPS TO REPRODUCE

- Use valid Alice Acme API identity: GET /api/invoices/3 with Accept: application/json on .16; 200 includes GLOBEX-CONFIDENTIAL-2001.
- Use valid Alice web identity: GET /invoices/3 and /documents/2/download on .16; 200 includes Globex confidential markers.

- Compare approved owner, foreign tenant and anonymous controls in ledgerly-read-acceptance matrix.
- Repeat API invoice 3 on .17 as Alice: 404; owner Carol gets its marker in matrix.

REMEDIATION

- Enforce InvoicePolicy::view and DocumentPolicy::download on every corresponding route/controller.
- Apply tenant-scoped route model binding or an equivalent global tenant scope with explicit authorization.
- Add regression tests for both directions, member roles and anonymous access; retain successful owner controls.

EVIDENCE

| FILE | SHA-256 | INTEGRITY |
|---|---|---|
| `evidence/appmap/laravel-20261110T152815-2883.json` | 95b51a184bcc8106… | PASS |
| `evidence/authz/ledgerly-read-acceptance-2026-11-10T153327+0000.json` | 539e5cf9bc63e5b9… | PASS |
| `evidence/http/20261110T153500-get-10.250.0.16-b2adb2.txt` | 6772703b447a91a4… | PASS |
| `evidence/http/20261110T153500-get-10.250.0.16-6f4f12.txt` | efc8586c7b58f008… | PASS |
| `evidence/http/20261110T153500-get-10.250.0.16-9252ca.txt` | fa067580b66756f5… | PASS |
| `evidence/http/20261110T153500-get-10.250.0.17-fbc938.txt` | a802a95810845d52… | PASS |
| `evidence/authz/20261110T153322-get-10.250.0.16-d7adb7.txt` | 2576b707ea9bcdc3… | PASS |
| `evidence/authz/20261110T153322-get-10.250.0.16-32df52.txt` | 0db2fb6aaf491669… | PASS |
| `evidence/authz/20261110T153322-get-10.250.0.16-d8bfe7.txt` | 46470f1e2baf5ea5… | PASS |
| `evidence/authz/20261110T153324-get-10.250.0.16-fcbb53.txt` | 1a3cbb491c9c0e8c… | PASS |
| `evidence/authz/20261110T153325-get-10.250.0.16-8a454d.txt` | 2fdaff8f85650f1b… | PASS |

F-003 MEDIUM · CWE-89 RESOLVED

# Search SQL injection bypasses the tenant filter

http://10.250.0.16:8000/search?q=

| SEVERITY | CVSS | CWE | STATUS |
| --- | --- | --- | --- |
| Medium | 6.5 | CWE-89 | Resolved |

## CVSS VECTOR

`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N`

## DESCRIPTION

SearchController reads q and interpolates it into DB::select at lines 13–14 (CWE-89, WSTG-INPV-05). In the approved experiment, Alice's normal no-match query returned no results; OR 1=1 returned all three seeded invoice summaries including GLOBEX-INV-2001; OR 1=0 returned none.

Fixed .17 is NOT affected by these tested payloads: separately approved continuation established valid Acme dashboard session and all three queries returned empty results. This SQL-injection allegation is rejected for the fixed build for the tested cases. Fixed source was unavailable; no broader clean-build assertion.

SQL construction is a distinct root cause from missing object authorization.

## IMPACT

A tenant account can alter SQL predicates to retrieve another tenant's invoice identifiers and customer names. Only the seeded invoice query was used; arbitrary tables, writes and availability effects were not tested.

## STEPS TO REPRODUCE

- Authenticate as Alice on .16 and verify Acme dashboard.
- GET /search?q=RV-NO-MATCH-ACCEPTANCE: results [].
- Send URL-encoded q=RV-NO-MATCH-ACCEPTANCE%' OR 1=1 -- : results include GLOBEX-INV-2001 and Hank Scorpio.
- q=RV-NO-MATCH-ACCEPTANCE%' OR 1=0 -- returns [].
- Review the approved browser run evidence for the exact URLs and responses.

REMEDIATION

Use bound parameters or Eloquent instead of SQL interpolation:

```
$rows = DB::select(
    'select id, number, customer from invoices where organization_id = ? and customer like ?',
    [$request->user()->organization_id, '%' . $q . '%']
);
```

Keep tenant filtering server-controlled and add regression tests for quotes, boolean payloads and cross-tenant markers.

EVIDENCE

| FILE | SHA-256 | INTEGRITY |
|---|---|---|
| evidence/appmap/laravel-20261110T152815-2883.json | 95b51a184bcc8106… | PASS |
| evidence/runs/20261110T152836-for-8f7d0c.txt | 5149048808a1838e… | PASS |
| evidence/runs/20261110T153604-python-3b0998.txt | 90844a0f9d3cee81… | PASS |
| evidence/browser/20261110T153601-ffe31b/summary.json | 5a9ba26938efad73… | PASS |
| evidence/browser/20261110T153601-ffe31b/requests.jsonl | bbbb4e0cef93f4a5… | PASS |
| evidence/runs/20261110T153822-python-679d08.txt | 4125b16dd65c84cb… | PASS |
| evidence/browser/20261110T153820-76f27d/summary.json | cd04e943f58471fc… | PASS |

07 · APPENDIX A

# Evidence integrity

SHA-256 of each evidence file at report time, and the audited command that produced exactly that content. **Pass**: unchanged since the sandbox produced it. **Not audited**:

hashed, but written outside the audited sandbox. **Code ref**: a location in the client's source code.

| FINDING | FILE | SHA-256 | PRODUCED BY | INTEGRITY |
|---|---|---|---|---|
| F-002 | evidence/runs/20261110T154550-cat-c9be74.txt | e2340150da7c0ebb94ac4198bdff2c86e31dbf4f8019d0c2aa8c7382fe29ebde | cat /src/rv-bench/rv-laravel-lab/app/Http/Controllers/Api/ProfileController.php; cat /src… 2026-11-10 15:45 UTC | PASS |
| F-002 | evidence/runs/20261110T155125-cat-40f59e.txt | 04aa239fa0479f9fa21aa0171b84dffaac60a5b7985477fb93533c160787cdd5 | cat app-does-not-exist 2>/dev/null; cat /src/rv-bench/rv-laravel-lab/app/Policies/Invoice… 2026-11-10 15:51 UTC | PASS |
| F-002 | evidence/http/20261110T154549-get-10.250.0.16-831372.txt | dd85062b686de9b0f49962822ed82c42e52f506e377e9bf22652ca7beb02e599 | http GET http://10.250.0.16:8000/api/me as bob-api 2026-11-10 15:45 UTC | PASS |
| F-002 | evidence/http/20261110T154550-get-10.250.0.17-bb1fd1.txt | 67ae8d07de9b0376f1926f0ef622f4efb5e5de7a686e60a9bc0c10dec9cbe2b1 | http GET http://10.250.0.17:8000/api/me as bob-api 2026-11-10 15:45 UTC | PASS |
| F-002 | evidence/http/20261110T154841-patch-10.250.0.16-342247.txt | 3b2b3d56b57933acdb2bdcfe7e4e775e32b257033f79a2d0825229f9222bbab9 | http PATCH http://10.250.0.16:8000/api/profile as bob-api 2026-11-10 15:48 UTC | PASS |
| F-002 | evidence/http/20261110T154858-get-10.250.0.16-448337.txt | ad13f79d49b9d694e4ed1c3b5d07f550355c7ff676a0cc037042da93520039f0 | http GET http://10.250.0.16:8000/api/me as bob-api 2026-11-10 15:48 UTC | PASS |
| F-002 | evidence/http/20261110T154841-patch-10.250.0.17-fd7fe4.txt | 5e4b9ea6eb463c923e2ca472f840503924f07da9386fec921b66d393bf6852d3 | http PATCH http://10.250.0.17:8000/api/profile as bob-api 2026-11-10 15:48 UTC | PASS |

| FINDING | FILE | SHA-256 | PRODUCED BY | INTEGRITY |
|---|---|---|---|---|
| F-002 | evidence/http/20261110T154858-get-10.250.0.17-ddaa7f.txt | 08b1f0b6617409739349e5a2d1f774376c1c0685e241cabda909046c07d2159d | http GET http://10.250.0.17:8000/api/me as bob-api 2026-11-10 15:48 UTC | PASS |
| F-002 | evidence/http/20261110T154907-patch-10.250.0.16-ac1250.txt | 0b4d18042c809a9d3679abf91497d078cad8db3a299c6567038bade175a60763 | http PATCH http://10.250.0.16:8000/api/profile as bob-api 2026-11-10 15:49 UTC | PASS |
| F-002 | evidence/http/20261110T154907-patch-10.250.0.17-fc70a2.txt | 1653762a6fe18c45e82f80302b6d5b94b8aa04cf4679c79ff3a67a5bb6de2e4d | http PATCH http://10.250.0.17:8000/api/profile as bob-api 2026-11-10 15:49 UTC | PASS |
| F-001 | evidence/appmap/laravel-20261110T152815-2883.json | 95b51a184bcc8106531bdebc69526e0ee92f8d5d6e0505a4a0a44d7122f03d5c | appmap laravel /src/rv-bench/rv-laravel-lab 2026-11-10 15:28 UTC | PASS |
| F-001 | evidence/authz/ledgerly-read-acceptance-2026-11-10T153327+0000.json | 539e5cf9bc63e5b9e00e27097641f073ba52b239c7e94b373d5920da4aa64d0a | authz run ledgerly-read-acceptance 2026-11-10 15:33 UTC | PASS |
| F-001 | evidence/http/20261110T153500-get-10.250.0.16-b2adb2.txt | 6772703b447a91a4946f819c3e21d1c100432fb3d42d0d69a5c6ef73cf7e1f92 | http GET http://10.250.0.16:8000/api/invoices/3 as alice-api 2026-11-10 15:35 UTC | PASS |
| F-001 | evidence/http/20261110T153500-get-10.250.0.16-6f4f12.txt | efc8586c7b58f0082f71e7c15482a5b6e17a811754f5e4b8ae5d126d198c3b77 | http GET http://10.250.0.16:8000/invoices/3 as alice-web 2026-11-10 15:35 UTC | PASS |
| F-001 | evidence/http/20261110T153500-get-10.250.0.16-9252ca.txt | fa067580b66756f5228d98bfdb1f351a16be6bdbc2ca7a7de1b9b7ed73f1911c | http GET http://10.250.0.16:8000/documents/2/download as alice-web 2026-11-10 15:35 UTC | PASS |

| FINDING | FILE | SHA-256 | PRODUCED BY | INTEGRITY |
|---|---|---|---|---|
| F-001 | evidence/http/20261110T153500-get-10.250.0.17-fbc938.txt | a802a95810845d52f7cfa04a308fa017edfeddec273228b215ba41b584cd7729 | http GET http://10.250.0.17:8000/api/invoices/3 as alice-api 2026-11-10 15:35 UTC | PASS |
| F-001 | evidence/authz/20261110T153322-get-10.250.0.16-d7adb7.txt | 2576b707ea9bcdc332ed5a87de21cbdb3c8e6d7d545a1758253621f208a236f8 | http GET http://10.250.0.16:8000/api/invoices/1 as carol-api 2026-11-10 15:33 UTC | PASS |
| F-001 | evidence/authz/20261110T153322-get-10.250.0.16-32df52.txt | 0db2fb6aaf49166987fbe2d52631d309118b04881e03066352c256f3c8e901e0 | http GET http://10.250.0.16:8000/api/invoices/3 as alice-api 2026-11-10 15:33 UTC | PASS |
| F-001 | evidence/authz/20261110T153322-get-10.250.0.16-d8bfe7.txt | 46470f1e2baf5ea54d8fbd6076d180a999a7740accad34117808a955ca5a262e | http GET http://10.250.0.16:8000/api/invoices/3 as bob-api 2026-11-10 15:33 UTC | PASS |
| F-001 | evidence/authz/20261110T153324-get-10.250.0.16-fcbb53.txt | 1a3cbb491c9c0e8ca0f178be1203e94512e25f7861867b3624f4ff7a02287354 | http GET http://10.250.0.16:8000/invoices/3 as alice-web 2026-11-10 15:33 UTC | PASS |
| F-001 | evidence/authz/20261110T153325-get-10.250.0.16-8a454d.txt | 2fdaff8f85650f1be1d0fb038b7351884a791230fc81756c25edf3eb115e50a4 | http GET http://10.250.0.16:8000/documents/2/download as alice-web 2026-11-10 15:33 UTC | PASS |
| F-003 | evidence/appmap/laravel-20261110T152815-2883.json | 95b51a184bcc8106531bdebc69526e0ee92f8d5d6e0505a4a0a44d7122f03d5c | appmap laravel /src/rv-bench/rv-laravel-lab 2026-11-10 15:28 UTC | PASS |
| F-003 | evidence/runs/20261110T152836-for-8f7d0c.txt | 5149048808a1838e8bdcceea5bc26c437c8ae8582820b6db4efb730cae415867 | for f in app/Http/Controllers/SearchController.php app/Http/Controllers/DocumentControlle… 2026-11-10 15:28 UTC | PASS |

| FINDING | FILE | SHA-256 | PRODUCED BY | INTEGRITY |
|---|---|---|---|---|
| F-003 | evidence/runs/20261110T153604-python-3b0998.txt | 90844a0f9d3cee81d3ae5bd07c1b1aa41b3d872acdc3497d803a915134462e84 | /opt/browser/bin/python /opt/kali-mcp/browser_runner.py /work/bench-acceptance-laravel/.b… 2026-11-10 15:36 UTC | PASS |
| F-003 | evidence/browser/20261110T153601-ffe31b/summary.json | 5a9ba26938efad73ef9ed973f1a026261b83c4ebeda9d3e7e679c29b5f1bca05 | /opt/browser/bin/python /opt/kali-mcp/browser_runner.py /work/bench-acceptance-laravel/.b… 2026-11-10 15:36 UTC | PASS |
| F-003 | evidence/browser/20261110T153601-ffe31b/requests.jsonl | bbbb4e0cef93f4a5a215060842be455c45d8f1cafa658ff293885e3cd1292124 | /opt/browser/bin/python /opt/kali-mcp/browser_runner.py /work/bench-acceptance-laravel/.b… 2026-11-10 15:36 UTC | PASS |
| F-003 | evidence/runs/20261110T153822-python-679d08.txt | 4125b16dd65c84cb6fb69f4f020181d7e2eda8afec014e6505e07c688b2bad28 | /opt/browser/bin/python /opt/kali-mcp/browser_runner.py /work/bench-acceptance-laravel/.b… 2026-11-10 15:38 UTC | PASS |
| F-003 | evidence/browser/20261110T153820-76f27d/summary.json | cd04e943f58471fc0f3863d057fbb99ac12e6e69096fb89ffc3992fc1033955f | /opt/browser/bin/python /opt/kali-mcp/browser_runner.py /work/bench-acceptance-laravel/.b… 2026-11-10 15:38 UTC | PASS |

# Activity summary

| MEASURE | VALUE |
| --- | --- |
| First / last activity | 2026-11-10 15:26 UTC / 2026-11-10 15:55 UTC |
| Commands run | 31 |
| Commands refused by policy | 1 |
| Evidence files recorded | 48 |
| Approvals requested / approved / denied | 7 / 7 / 0 |
| Emergency halts | 0 |
| Scope changes | 2 |
| Results triaged as false positives | 0 |
| Results merged as duplicates | 0 |