TEST REPORT · SECURITY / PENETRATION TEST

● 1 HIGH (FIXED) · 4 MEDIUM OPEN

# Acme Ledger web app and API

| | |
|---|---|
| Authorisation | Signed test agreement, 6 Oct 2026; scope and window agreed with the CTO |
| Scope | `app.staging.acme-ledger.example`, customer portal, Public API 2.4 (all endpoints) |
| Approach | Grey box: test accounts for 5 roles in 2 test tenants, API documentation, no source code |
| Method | OWASP WSTG 4.2, ASVS 4.0.3 Level 2 (selected), OWASP API Security Top 10 2023 |
| Test window | 12 Oct 2026 – 16 Oct 2026 · retest 23 Oct 2026 |
| Tester | Tomasz Kordiak |

## Contents

1. Summary
2. Findings by severity
3. Defects
4. Observations
5. Findings
6. Authorization matrix
7. Test checklist
8. Retest
9. Scope and rules of engagement
10. Timeline
11. Method and limits

## Summary

The application has a solid baseline: 82 of 91 applicable checks passed, TLS, cookies, password storage and most authorization are done right, and there are no critical issues. The most serious finding was an authorization gap on two invoice endpoints that let one customer read another customer's invoices (SEC-01). It was fixed before the 4.2 release and the fix was verified.

Four Medium findings remain open with fixes planned: stored XSS in the portal, no login rate limiting, long-lived sessions and CSV formula injection.

> **Release recommendation**
>
> No open finding blocks release 4.2. Fix SEC-02, SEC-03 and SEC-05 in 4.2.1 (within 2 weeks), SEC-04 in 4.3.

## Findings by severity

| 0 | 1 | 4 | 4 | 94 |
|---|---|---|---|---|
| Critical | High | Medium | Low | Checks performed |

**2** Fixed and retested

| ID | FINDING | SEVERITY | CVSS | STATUS |
|---|---|---|---|---|
| SEC-01 | Invoice PDF and resend endpoints don't check the tenant (BOLA) | High | 7.1 | Fixed · retested |
| SEC-02 | Stored cross-site scripting in invoice notes (customer portal) | Medium | 5.4 | Open |
| SEC-03 | No rate limiting or lockout on login | Medium | 5.3 | Open |
| SEC-04 | Sessions stay valid after logout and password change | Medium | 4.8 | Open |
| SEC-05 | CSV export allows formula injection | Medium | 4.6 | Open |
| SEC-06 | Missing Content-Security-Policy and Permissions-Policy headers | Low | – | Open |
| SEC-07 | Password reset reveals whether an email has an account | Low | 3.7 | Open |
| SEC-08 | Stack traces in 500 responses | Low | 3.7 | Fixed · retested |
| SEC-09 | Invite links don't expire after use | Low | 3.1 | Open |

| SEVERITY | OPEN | FIXED | TOTAL |
|---|---|---|---|
| Critical | – | – | **0** |
| High | – | 1 | **1** |
| Medium | 4 | – | **4** |

| SEVERITY | OPEN | FIXED | TOTAL |
|---|---|---|---|
| Low | 3 | 1 | **4** |

## Defects Jira tickets for each finding

| KEY | SUMMARY | SEVERITY | STATUS | COMPONENT | FOUND BY | OWNER | CREATED |
|---|---|---|---|---|---|---|---|
| ACME-531 | [SEC-01] Invoice PDF and resend endpoints don't check the tenant (BOLA) | High | Fixed | GET /invoices/{id}/pdf | – | Backend | 13 Oct |
| ACME-532 | [SEC-02] Stored cross-site scripting in invoice notes (customer portal) | Medium | Open | Invoice **Notes** field rendered in the customer portal | – | Frontend | 14 Oct |
| ACME-533 | [SEC-03] No rate limiting or lockout on login | Medium | Open | Web app | – | Backend | 15 Oct |
| ACME-534 | [SEC-04] Sessions stay valid after logout and password change | Medium | Open | Web app | – | Frontend | 16 Oct |
| ACME-535 | [SEC-05] CSV export allows formula injection | Medium | Open | Web app | – | Backend | 16 Oct |

| KEY | SUMMARY | SEVERITY | STATUS | COMPONENT | FOUND BY | OWNER | CREATED |
|---|---|---|---|---|---|---|---|
| `ACME-536` | [SEC-06] Missing Content-Security-Policy and Permissions-Policy headers | Low | Open | Web app | – | Frontend | 16 Oct |
| `ACME-537` | [SEC-07] Password reset reveals whether an email has an account | Low | Open | Web app | – | Backend | 16 Oct |
| `ACME-538` | [SEC-08] Stack traces in 500 responses | Low | Fixed | Web app | – | Frontend | 16 Oct |
| `ACME-539` | [SEC-09] Invite links don't expire after use | Low | Open | Web app | – | Backend | 16 Oct |

## Observations not vulnerabilities

| ID | AREA | OBSERVATION | IMPACT | SUGGESTED ACTION |
|---|---|---|---|---|
| `OBS-01` | Positive | Tenant isolation holds on all other API operations, including filters, pagination cursors and exports. | Positive | Keep the negative tests added in rc3 for every `{id}` route. |
| `OBS-02` | Dependencies | `npm audit` and `pip-audit`: no known critical or high vulnerabilities; 3 moderate in dev dependencies. | Low | Update in the next dependency cycle. |
| `OBS-03` | Logging | Failed logins and permission denials are logged, but nobody gets alerted. | Detection | Alert on spikes (ties in with SEC-03). |

| ID | AREA | OBSERVATION | IMPACT | SUGGESTED ACTION |
|---|---|---|---|---|
| `OBS-04` | MFA | MFA is enforced for admins but optional for Finance, who can issue refunds. | Medium | Require MFA for any role that moves money. |
| `OBS-05` | Secrets | Webhook secrets are shown again in the UI after creation. | Low | Show once, then mask (like API secrets). |
| `OBS-06` | Process | No security.txt or vulnerability disclosure contact. | Low | Publish `/.well-known/security.txt`. |

## Findings CVSS 3.1 base scores

### High SEC-01 Invoice PDF and resend endpoints don't check the tenant (BOLA)

**CVSS 3.1** 7.1 · `AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N`

**Category** OWASP API1:2023 Broken Object Level Authorization · CWE-639

**Affected** `GET /invoices/{id}/pdf`, `POST /invoices/{id}/send`

**Description** `GET /invoices/{id}` correctly returns `404` for another tenant's invoice, but the PDF and resend endpoints only check that the caller is authenticated. Invoice IDs appear in links in emailed invoices, so they are not secret.

**Reproduction**

- As a tenant A user, take an invoice ID of tenant B (test tenants).
- `GET /invoices/{id}/pdf` with tenant A's token → `200` and tenant B's PDF.
- `POST /invoices/{id}/send` → tenant B's customer receives the invoice again.

**Impact** Any customer can read other customers' invoices and trigger emails on their behalf.

**Remediation** Shared authorization layer for every `{id}` route; negative tests per endpoint.

**Status** Fixed in 4.2.0-rc3 · retested 23 Oct 2026 · both endpoints return `404`.

### Medium SEC-02 Stored cross-site scripting in invoice notes (customer portal)

**CVSS 3.1** 5.4 · `AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N`

**Category** OWASP A03:2021 Injection · CWE-79

**Affected** Invoice **Notes** field rendered in the customer portal

**Description** HTML in Notes is escaped in the back office but rendered as HTML in the portal. A harmless test payload executed in the customer's browser.

**Remediation** Escape on output in the portal template; add a Content-Security-Policy (SEC-06).

**Status** Open · planned for 4.2.1

### Medium SEC-03 No rate limiting or lockout on login

| | |
|---|---|
| CVSS 3.1 | 5.3 · `AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N` |
| Category | OWASP API4:2023 Unrestricted Resource Consumption · CWE-307 |
| Description | 200 failed logins for one test account in 60 seconds were all processed (test limited to our own account). |
| Remediation | Rate limit per account and IP, progressive delay after 5 failures, alerting on spikes. |
| Status | Open · planned for 4.2.1 |

### Medium SEC-04 Sessions stay valid after logout and password change

| | |
|---|---|
| CVSS 3.1 | 4.8 · `AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N` |
| Category | OWASP A07:2021 Identification and Authentication Failures · CWE-613 |
| Description | Access tokens are JWTs valid for 24 h without server-side revocation. |
| Remediation | 15-minute access tokens with refresh tokens; revoke on password change and logout. |
| Status | Open · design agreed, 4.3 |

### Medium SEC-05 CSV export allows formula injection

| | |
|---|---|
| CVSS 3.1 | 4.6 · `AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N` |
| Category | CWE-1236 Improper Neutralization of Formula Elements in a CSV File |
| Description | A customer name starting with `=` is exported unchanged; opening the CSV in a spreadsheet evaluates it as a formula. |
| Remediation | Prefix cells starting with `= + - @` with an apostrophe in all CSV exports. |
| Status | Open · 4.2.1 |

### Low SEC-06 Missing Content-Security-Policy and Permissions-Policy headers

| | |
|---|---|
| Description | Web app and portal send HSTS and X-Content-Type-Options, but no CSP or Permissions-Policy. |
| Remediation | CSP in report-only mode first, then enforce. Would have limited SEC-02. |

### Low SEC-07 Password reset reveals whether an email has an account

| | |
|---|---|
| CVSS 3.1 | 3.7 · `AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N` |
| Description | `POST /auth/reset` returns `404 User not found` for unknown emails. |
| Remediation | Always return `200` with the same message. |

Low SEC-08 **Stack traces in 500 responses**

| | |
|---|---|
| CVSS 3.1 | 3.7 · `AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N` |
| Description | Malformed JSON in `POST /customers` returned a stack trace with library versions. |
| Status | Fixed in 4.2.0-rc3 · retested |

Low SEC-09 **Invite links don't expire after use**

| | |
|---|---|
| CVSS 3.1 | 3.1 · `AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N` |
| Description | An accepted invite link still shows the sign-up form (account creation is blocked, but the email is shown). |
| Remediation | Invalidate the token on acceptance. |

## Authorization matrix

| ENDPOINT | ADMIN | FINANCE | ACCOUNTANT | SALES | VIEWER | OTHER TENANT | NO TOKEI |
|---|---|---|---|---|---|---|---|
| `GET /invoices` | ✓ | ✓ | ✓ | ✓ | ✓ | × | × |
| `GET /invoices/{id}` | ✓ | ✓ | ✓ | ✓ | ✓ | × | × |
| `GET /invoices/{id}/pdf` | ✓ | ✓ | ✓ | ✓ | ✓ | ! | × |
| `POST /invoices` | ✓ | ✓ | × | ✓ | × | × | × |
| `POST /invoices/{id}/send` | ✓ | ✓ | × | ✓ | × | ! | × |
| `DELETE /invoices/{id}` | ✓ | × | × | × | × | × | × |
| `POST /payments` | ✓ | ✓ | × | × | × | × | × |
| `POST /payments/{id}/refund` | ✓ | ✓ | × | × | × | × | × |
| `GET /customers` | ✓ | ✓ | ✓ | ✓ | ✓ | × | × |
| `GET /customers/export.csv` | ✓ | ✓ | × | ✓ | × | × | × |
| `GET /reports/revenue` | ✓ | ✓ | ✓ | × | ✓ | × | × |

| ENDPOINT | ADMIN | FINANCE | ACCOUNTANT | SALES | VIEWER | OTHER TENANT | NO TOKEI |
|---|---|---|---|---|---|---|---|
| `POST /users/invite` | ✓ | × | × | × | × | × | × |
| `PATCH /settings/company` | ✓ | × | × | × | × | × | × |
| `POST /webhooks` | ✓ | × | × | × | × | × | × |
| `GET /audit-events` | ✓ | × | ✓ | × | × | × | × |

15 endpoints × 7 actors = 105 authorization checks. ✓ allowed as designed, × denied as designed, ! finding (SEC-01, fixed).

## Test checklist 94 checks · 82 pass · 9 fail · 3 n/a

| CATEGORY | CHECKS | PASS | FAIL | N/A |
|---|---|---|---|---|
| Information gathering | 7 | 7 | – | – |
| Configuration and deployment | 10 | 8 | 2 | – |
| Authentication | 12 | 8 | 3 | 1 |
| Authorization | 10 | 9 | 1 | – |
| Session management | 8 | 7 | 1 | – |
| Input validation | 14 | 11 | 2 | 1 |
| Business logic | 9 | 9 | – | – |
| Files and uploads | 6 | 6 | – | – |
| API specific | 8 | 8 | – | – |
| Cryptography | 5 | 5 | – | – |
| Client side | 5 | 4 | – | 1 |

### Information gathering

| ID | CHECK | RESULT | FINDING |
|---|---|---|---|
| `INF-01` | Fingerprint web server and frameworks | Pass | – |

| ID | CHECK | RESULT | FINDING |
|---|---|---|---|
| INF-02 | Review robots.txt and sitemap for hidden paths | Pass | – |
| INF-03 | Identify entry points (UI and API) | Pass | – |
| INF-04 | Map application architecture | Pass | – |
| INF-05 | Review client-side code for secrets | Pass | – |
| INF-06 | Check for exposed `.git` or backups | Pass | – |
| INF-07 | Enumerate subdomains in scope | Pass | – |

### Configuration and deployment

| ID | CHECK | RESULT | FINDING |
|---|---|---|---|
| CON-01 | TLS versions and ciphers | Pass | – |
| CON-02 | HSTS present and preloaded | Pass | – |
| CON-03 | Security headers | Fail | SEC-06 |
| CON-04 | HTTP methods allowed | Pass | – |
| CON-05 | Admin interfaces exposed | Pass | – |
| CON-06 | Default credentials | Pass | – |
| CON-07 | Directory listing | Pass | – |
| CON-08 | Error handling leaks details | Fail | SEC-08 |
| CON-09 | CORS policy | Pass | – |
| CON-10 | Cloud storage permissions | Pass | – |

### Authentication

| ID | CHECK | RESULT | FINDING |
|---|---|---|---|
| AUT-01 | Credentials over encrypted channel | Pass | – |
| AUT-02 | Default and weak passwords | Pass | – |
| AUT-03 | Lockout mechanism | Fail | SEC-03 |
| AUT-04 | Bypass authentication schema | Pass | – |

| ID | CHECK | RESULT | FINDING |
|---|---|---|---|
| AUT-05 | Remember-me | N/A | – |
| AUT-06 | Browser cache of sensitive pages | Pass | – |
| AUT-07 | Password policy | Pass | – |
| AUT-08 | Password reset | Fail | SEC-07 |
| AUT-09 | MFA enforcement for admins | Pass | – |
| AUT-10 | SSO (SAML) assertion validation | Pass | – |
| AUT-11 | Account enumeration on login | Pass | – |
| AUT-12 | Invite flow | Fail | SEC-09 |

### Authorization

| ID | CHECK | RESULT | FINDING |
|---|---|---|---|
| AUT-01 | Path traversal / file include | Pass | – |
| AUT-02 | Bypass authorization schema | Pass | – |
| AUT-03 | Privilege escalation between roles | Pass | – |
| AUT-04 | Object-level authorization (BOLA) | Fail | SEC-01 |
| AUT-05 | Function-level authorization | Pass | – |
| AUT-06 | Tenant isolation in filters | Pass | – |
| AUT-07 | Tenant isolation in pagination cursors | Pass | – |
| AUT-08 | Tenant isolation in exports | Pass | – |
| AUT-09 | Tenant isolation in webhooks | Pass | – |
| AUT-10 | Mass assignment of `tenantId` / `role` | Pass | – |

### Session management

| ID | CHECK | RESULT | FINDING |
|---|---|---|---|
| SES-01 | Session token randomness | Pass | – |
| SES-02 | Cookie attributes | Pass | – |

| ID | CHECK | RESULT | FINDING |
|---|---|---|---|
| SES–03 | Session fixation | Pass | – |
| SES–04 | CSRF protection | Pass | – |
| SES–05 | Logout invalidates session | Fail | SEC–04 |
| SES–06 | Session timeout | Pass | – |
| SES–07 | Token in URL | Pass | – |
| SES–08 | Concurrent sessions | Pass | – |

### Input validation

| ID | CHECK | RESULT | FINDING |
|---|---|---|---|
| INP–01 | Reflected XSS | Pass | – |
| INP–02 | Stored XSS | Fail | SEC–02 |
| INP–03 | DOM XSS | Pass | – |
| INP–04 | SQL injection | Pass | – |
| INP–05 | NoSQL injection | N/A | – |
| INP–06 | Command injection | Pass | – |
| INP–07 | Server-side template injection | Pass | – |
| INP–08 | SSRF via webhook URL | Pass | – |
| INP–09 | SSRF via file import URL | Pass | – |
| INP–10 | XML external entities (UBL import) | Pass | – |
| INP–11 | HTTP parameter pollution | Pass | – |
| INP–12 | CSV formula injection | Fail | SEC–05 |
| INP–13 | Header injection in emails | Pass | – |
| INP–14 | Open redirect | Pass | – |

### Business logic

| ID | CHECK | RESULT | FINDING |
|---|---|---|---|
| BUS-01 | Negative amounts and quantities | Pass | – |
| BUS-02 | Overpayment and refunds above paid | Pass | – |
| BUS-03 | Race condition: double payment | Pass | – |
| BUS-04 | Race condition: double refund | Pass | – |
| BUS-05 | Invoice number manipulation | Pass | – |
| BUS-06 | Workflow bypass (send cancelled invoice) | Pass | – |
| BUS-07 | Discount over 100% | Pass | – |
| BUS-08 | Currency switch after payment | Pass | – |
| BUS-09 | Abuse of free trial limits | Pass | – |

### Files and uploads

| ID | CHECK | RESULT | FINDING |
|---|---|---|---|
| FIL-01 | File type validation server-side | Pass | – |
| FIL-02 | File size limit | Pass | – |
| FIL-03 | Malicious file content (polyglot) | Pass | – |
| FIL-04 | Uploaded files served from separate domain | Pass | – |
| FIL-05 | Download links expire | Pass | – |
| FIL-06 | Path in file name | Pass | – |

### API specific

| ID | CHECK | RESULT | FINDING |
|---|---|---|---|
| API-01 | API9 inventory: undocumented endpoints | Pass | – |
| API-02 | API3 excessive data exposure | Pass | – |
| API-03 | API4 rate limiting on API | Pass | – |
| API-04 | API6 sensitive business flows | Pass | – |

| ID | CHECK | RESULT | FINDING |
|---|---|---|---|
| `API-05` | API8 misconfiguration | Pass | – |
| `API-06` | API10 unsafe consumption of webhooks | Pass | – |
| `API-07` | Versioning: v1 endpoints still reachable | Pass | – |
| `API-08` | Error messages consistent | Pass | – |

### Cryptography

| ID | CHECK | RESULT | FINDING |
|---|---|---|---|
| `CRY-01` | Password storage algorithm | Pass | – |
| `CRY-02` | Secrets in responses | Pass | – |
| `CRY-03` | Webhook signature algorithm | Pass | – |
| `CRY-04` | JWT algorithm and key handling | Pass | – |
| `CRY-05` | Random number generation for tokens | Pass | – |

### Client side

| ID | CHECK | RESULT | FINDING |
|---|---|---|---|
| `CLI-01` | Clickjacking protection | Pass | – |
| `CLI-02` | Sensitive data in local storage | Pass | – |
| `CLI-03` | Third-party scripts | Pass | – |
| `CLI-04` | Subresource integrity on CDN scripts | N/A | – |
| `CLI-05` | postMessage handling | Pass | – |

## Retest

| FINDING | FIX | RETEST 23 OCT | RESULT |
|---|---|---|---|
| `SEC-01` | Tenant check moved to a shared middleware | Both endpoints `404` for other tenants; 15 negative tests added | Fixed |

| FINDING | FIX | RETEST 23 OCT | RESULT |
|---|---|---|---|
| `SEC-08` | Generic error body in production | Malformed JSON → `400` with message only | Fixed |
| `SEC-02 – SEC-07, SEC-09` | Planned for 4.2.1 / 4.3 | Retest scheduled after the fixes | Pending |

## Scope and rules of engagement

| | |
|---|---|
| **In scope** | Web app, customer portal, Public API 2.4, SSO login, file upload, webhooks |
| **Out of scope** | Production, denial-of-service, social engineering, payment provider, office network, physical |
| **Accounts** | 2 test tenants × 5 roles, 1 SSO test user, 3 API clients |
| **Limits** | Max 10 requests/s for automated scans; brute-force tests limited to own test accounts |
| **Data** | Synthetic data only; no production data accessed |
| **Contacts** | CTO (escalation), on-call engineer (availability during the window) |
| **Critical findings** | Reported the same day by phone and email (SEC-01 reported 13 Oct, 15:20) |

## Timeline

| DATE | ACTIVITY |
|---|---|
| 6 Oct | Scope, authorisation and test accounts agreed |
| 12 Oct | Reconnaissance, configuration, authentication |
| 13 Oct | Authorization testing; SEC-01 found and reported the same day |
| 14 Oct | Input validation, business logic |
| 15 Oct | Files, API-specific, cryptography, client side |
| 16 Oct | Verification of findings, draft report |

| DATE | ACTIVITY |
| --- | --- |
| 23 Oct | Retest of fixes in rc3, final report |

## Method and limits

Manual testing supported by Burp Suite and OWASP ZAP; automated scans were rate-limited to avoid load on staging. A penetration test is a point-in-time check of the agreed scope and does not prove the absence of vulnerabilities.

Evidence (requests, responses, screenshots) is stored encrypted, shared only with the named contacts and deleted 90 days after the final retest.

Sample report. Acme Ledger, its data, people and defects are fictional. Your report shows your product, your tickets and your tools.

More sample reports · Book a 15-minute call