ATVORA

SAMPLE DOCUMENT

Evidence Pack

Engagement: *Illustrative engagement, shown as delivered*
Client: *An invented subscription business, professional services*
Application: *Client portal and subscription billing*
Repository: *Private repository*
Scope pinned to commit: *a1b2c3d*
Package: *Rescue and Harden*
Dates: *26 May 2026 to 4 June 2026*

What this document is

> A record of the review and verification work performed on an application at a pinned commit. It is not a certification, an audit, or a penetration test. The engagement on this page is illustrative: the client is invented, and the findings are drawn from the failures we keep finding in real AI built codebases. The structure, the checks, and the standard of evidence are exactly what ships with every Atvora delivery.

Checks performed

Secrets scan, dependency audit, authentication and authorisation review, input handling review, error handling review, deployment configuration review, and an adversarial second model review pass.

Findings and fixes

SEVERITY	FINDING	FIX APPLIED	COMMIT
Critical	The session identity was trusted from a client supplied value, so a request could be made on behalf of any user by substituting their id.	Session verified server side with the auth provider on every request; the user id is derived from the verified session, never from the request body.	4f1c9ab
Critical	The subscription tier was writable directly from a client request, so a free account could set itself to paid without payment.	Plan state removed from client writable fields; entitlement is now set only by a signed webhook from the payment provider after a confirmed charge.	b7e22d0
High	Database row level security was disabled, so any signed in account could read and write other tenants' records.	Row level security enabled with per tenant policies on every user data table; cross tenant access denied by default.	9c0f3e1
High	Live payment and email provider keys were present in the git history.	Keys rotated, moved to server side environment variables, and secret scanning added to the delivery pipeline; the exposure window was documented for the client.	2a55d8c
Medium	Several write endpoints trusted the shape of client input without validation.	Schema validation added on all write endpoints; invalid requests are rejected before reaching the database.	e3b1740
Medium	Failures returned stack traces and internal file paths to the browser.	Generic error responses to clients; diagnostic detail retained in server logs only.	c81aa92
Low	Several dependencies carried published security advisories.	Upgraded to patched versions; a dependency audit now runs in the pipeline on every change.	70d9f5b

Verification

CHECK	RESULT
A request cannot act as another user, tested with substituted identities	*Pass*
A free account cannot reach a paid entitlement without a confirmed payment	*Pass*
Cross tenant read and write are denied by default	*Pass*
Secret scan over the working tree and git history	*Clean, prior keys rotated*
Dependency audit	*No known high or critical advisories*
Authentication and billing flows, exercised end to end against the provider sandbox	*Pass*
Production build and deployment	*Succeeded, preview promoted to production*

Deployment record

Hosted on Vercel. Environment variables held in the platform, never in the repository.
Database on managed Postgres with row level security enforced.
Payment webhooks verified by signature before any entitlement change.
Preview deployment reviewed, then promoted to production on 4 June 2026.
Custom domain with automatic TLS.

Residual risk statement

1. This record covers the application at the pinned commit only. Changes merged afterward are out of scope.
2. Third party services for payment, email, and hosting are trusted to honour their own security; their internals were not reviewed.
3. Load and performance testing beyond functional verification was not part of this engagement.
4. New dependency advisories will appear over time and require ongoing updates; a Care Plan covers this if engaged.
5. This is a record of work performed and verified. It is not a certification, an audit, or a penetration test.

Changes made after the pinned commit are outside the scope of this document.

Signed: Alexander Russell, Atvora
Date: 4 June 2026
atvora.com