

DEAL PACK SECURITY REPORT

Harbor Ledger — prepared for Initech

Package: Deal Pack · Valid until Jan 14, 2027. Mapped to SOC 2 (2017 TSC) and ISO/IEC 27001:2022 Annex A.

Sample report. Harbor Ledger, Initech and every finding here are fictional: a demo deal run through the same report builder as a real one.

Areas checked

5 of 7

1 not in package

Open critical / high

3

Expert-reviewed critical / high

100%

Questions answered

7 of 9

Summary

Automated checks found 10 confirmed issues: 1 critical, 2 high, 5 medium, 2 low. Expert-verified: 4; rule: 2; AI + sample re-check: 4.

Scope & coverage — what this review covers and what it doesn't

5 of 6 areas checked in full. Not in the Deal Pack package: Cloud.

Area	What was checked	Result	Not checked
Code	Static analysis of the source code for common vulnerability patterns. harborledger/platform	Checked	Business logic; Authorization design
Secrets	Code and full git history scanned for credentials and keys. harborledger/platform	Checked	Secrets outside the repository
Dependencies	Lockfiles checked against published advisories; for Gradle without a lockfile, the declared versions. harborledger/platform · 386 components	Checked	Dependencies without a lockfile
Containers & IaC	Dockerfiles, Terraform, Kubernetes and Helm configuration; public base images on Docker Hub and GitHub Container Registry. harborledger/platform	Checked	—
Website	TLS, security headers and a passive scan of the public pages of verified domains: no attacks, no login. app.harborledger.example · 41 pages	Checked	Pages behind login; Active attacks
Cloud	—	Not in package	—
Organization	Security measures backed by documents you provide or declared in questionnaire answers. 6 measures: 2 with documents, 3 declared	Partial	How the measures work in practice; 1 measure without data

Not covered by this review

Penetration test · Authenticated app testing · Architecture & threat model · Physical & HR security

Findings by area

Code

Severity	Finding	Review	Status
HIGH	SQL query built from user input	Expert-verified	Open
MEDIUM	Session cookie without the Secure flag	AI + sample re-check	Open

Also found: 1 low. Low and informational findings are counted, not listed.

HIGH SQL query built from user input

semgrep · javascript.express.security.audit.sqli · CWE-89 · src/invoices/invoice-search.service.ts:58

Expert-verified

The invoice search pastes the query string into SQL without parameters.

Expert note: Real issue: the invoice search builds SQL from the request. Use a parameterised query; the re-scan confirms the fix.

How to fix: Pass the reference as a query parameter: `db.query("SELECT * FROM invoices WHERE customer_ref = $1", [query.ref])`.

Controls: SOC 2 CC6.1, SOC 2 CC7.1, ISO 27001 A.8.28

MEDIUM Session cookie without the Secure flag

semgrep · javascript.express.security.cookie-missing-secure · CWE-614 · src/auth/session.middleware.ts:21

AI + sample re-check

The session cookie is also sent over plain HTTP.

How to fix: Add ``secure: true`` to the cookie options in `src/auth/session.middleware.ts`.

Controls: SOC 2 CC7.1, ISO 27001 A.8.28

Secrets

No confirmed issues.

Containers & IaC, website and dependency findings are listed in their own sections below.

Containers & IaC

Dockerfiles, Terraform, Kubernetes and Helm configuration checked for misconfigurations; public base images (Docker Hub, GitHub Container Registry) checked for high and critical vulnerabilities that have a fix. Private images and docker-compose files are not checked (trivy).

No confirmed issues.

Website — passive check

TLS configuration and HTTP security headers of the verified domain were checked. Public pages of app.harborledger.example were checked with passive rules only: no attacks were sent, no login was used and robots.txt was respected.

Severity	Finding	Pages	Review	Status
TLS and HTTP headers · 1				
MEDIUM	Content-Security-Policy header is missing	—	Rule	Open

Also found: 1 low. Low and informational findings are counted, not listed.

MEDIUM Content-Security-Policy header is missing

headers · headers.csp-missing · CWE-693 · app.harborledger.example Rule

https://app.harborledger.example/ answers without a Content-Security-Policy header.

How to fix: Send a Content-Security-Policy header; start with default-src 'self' and add the hosts the app loads from.

Controls: SOC 2 CC6.6, ISO 27001 A.8.26

Dependencies & SBOM

Lockfiles checked against published advisories (OSV).

5 advisories in 3 installed package versions; each has a fixed version to upgrade to. The table lists one row per package, with the version that fixes its advisories.

Severity	Package	Advisories	Upgrade to	Review
CRITICAL	lodash@4.17.20	2 (1 critical, 1 high)	4.17.21	Expert-verified
MEDIUM	follow-redirects@1.14.7	2 (2 medium)	1.15.4	AI + sample re-check
MEDIUM	minimist@1.2.5	1	1.2.6	AI + sample re-check

CRITICAL lodash@4.17.20 x2

npm · package-lock.json Expert-verified

Upgrade to 4.17.21, which fixes every advisory below.

- CRITICAL** Command injection in lodash 4.17.20 GHSA-35jh-r3h4-6jhm
- HIGH** Prototype pollution in lodash 4.17.20 GHSA-p6mc-m468-83gw

Expert note: Upgrade lodash to 4.17.21: the invoice export renders templates with it.

Expert note: Fixed by the same lodash upgrade.

How to fix: Bump lodash to 4.17.21 or later.

Controls: SOC 2 CC7.1, ISO 27001 A.8.8

MEDIUM follow-redirects@1.14.7 x2

npm · package-lock.json AI + sample re-check

Upgrade to 1.15.4, which fixes every advisory below.

- **MEDIUM** Exposure of the Authorization header in follow-redirects 1.14.7 GHSA-pw2r-vq6v-hr8c
- **MEDIUM** Improper URL handling in follow-redirects 1.14.7 GHSA-jchw-25xp-jwwc

How to fix: Bump follow-redirects to 1.15.4 or later; it fixes both advisories.

Controls: SOC 2 CC7.1, ISO 27001 A.8.8

MEDIUM minimist@1.2.5

npm · package-lock.json AI + sample re-check

Upgrade to 1.2.6, which fixes every advisory below.

- **MEDIUM** Prototype pollution in minimist 1.2.5 GHSA-xvch-5gv4-984h

How to fix: Bump minimist to 1.2.6 or later.

Controls: SOC 2 CC7.1, ISO 27001 A.8.8

A software bill of materials (SBOM) lists 386 third-party components in 1 repository; 3 of them have known vulnerabilities, listed above.

Ecosystem	Components	With known vulnerabilities	
npm	386	3	

Repository	Commit	Components	With known vulnerabilities
harborledger/platform	3f9a1c2	386	3

The SBOM is a CycloneDX JSON file per repository and is not attached to this report: Harbor Ledger can download it in DealReady and share it on request.

Organizational measures

2 of 6 measures backed by a document, 3 declared by the vendor, 1 without data.

Measure	Basis	Valid until
MFA on all staff accounts	Document provided	Apr 4, 2027
Offboarding within 24 hours	No data	—
Backups with a tested restore	Document provided	Jan 4, 2027
Centralized logging	Declared by vendor	—
Incident response plan	Declared by vendor	—
Encryption at rest	Declared by vendor	—

“Document provided” means Harbor Ledger supplied a current document, such as a screenshot of a setting or a written procedure; DealReady did not audit the process it describes. “Declared by vendor” rests on an approved questionnaire answer, without a document.

Control mapping

SOC 2

Control	Title	Status
CC6.1	Logical access security over protected information assets	Issues: 2
CC6.6	Protection against threats from outside system boundaries	Issues: 2
CC6.7	Protection of data in transmission	No issues
CC7.1	Detection of vulnerabilities and configuration changes	Issues: 7

ISO/IEC 27001:2022

Control	Title	Status
A.5.17	Authentication information	No issues
A.8.8	Management of technical vulnerabilities	Issues: 5
A.8.9	Configuration management	No issues
A.8.12	Data leakage prevention	Issues: 1
A.8.24	Use of cryptography	No issues
A.8.26	Application security requirements	Issues: 2
A.8.28	Secure coding	Issues: 2

Evidence on file · Questionnaire

- No secrets found in the repository · valid until Jan 14, 2027
- Code scanned with semgrep on every release · valid until Jan 14, 2027

Customer questionnaire. Answered: 7 of 9 questions.

Method & limits

Checks performed

- **Secrets in the repository.** Code and commit history scanned for credentials and keys (gitleaks).
- **Source code.** Static analysis rules for common vulnerability patterns (semgrep).
- **Open-source dependencies.** Lockfiles checked against published advisories (OSV).
- **Containers and infrastructure as code.** Dockerfiles, Terraform, Kubernetes and Helm configuration checked for misconfigurations; public base images (Docker Hub, GitHub Container Registry) checked for high and critical vulnerabilities that have a fix. Private images and docker-compose files are not checked (trivy).
- **TLS configuration.** Certificate and protocol versions of the verified domain.
- **HTTP security headers.** HSTS, CSP and other response headers of the verified domain.

- **Website — passive check.** Public pages of app.harborledger.example checked with OWASP ZAP baseline rules for cookies, cross-origin access (CORS), response headers, information leaks, version disclosure and known-vulnerable JavaScript libraries. Passive only: no attacks were sent, no login was used and robots.txt was respected; the number of pages and the scan time are limited. Pages behind a login are not checked (zap).

Review labels

Expert-verified	A DealReady security expert reviewed the finding and confirmed it.
Rule	The result of a deterministic check (TLS, HTTP headers): a fact, not a judgement.
AI + sample re-check	Confirmed by AI triage: medium and lower severity, or a vulnerable package version with a known fix; the expert re-checks a sample.
Vendor-declared	The vendor accepted the risk before an expert reviewed the finding.
Risk accepted by vendor	The vendor decided to accept the risk; the reason is given with the finding.
Acceptable risk (expert)	The expert confirmed the finding and judged its risk acceptable.
Fixed — not yet confirmed	The vendor marked the finding as fixed; no later scan has checked it yet.
Fixed — confirmed by a re-scan	A later scan of the same target no longer finds the issue.

Limits

- Low and informational findings are counted per area, not listed.
 - Findings nobody has reviewed yet are counted on the first page; they are not listed and not counted as resolved.
 - Areas outside the package or without results are marked in Scope & coverage.
- Automated scanning with expert validation; this is not a penetration test and does not certify compliance.