PRODUCTION READINESS / EVIDENCE RECORD

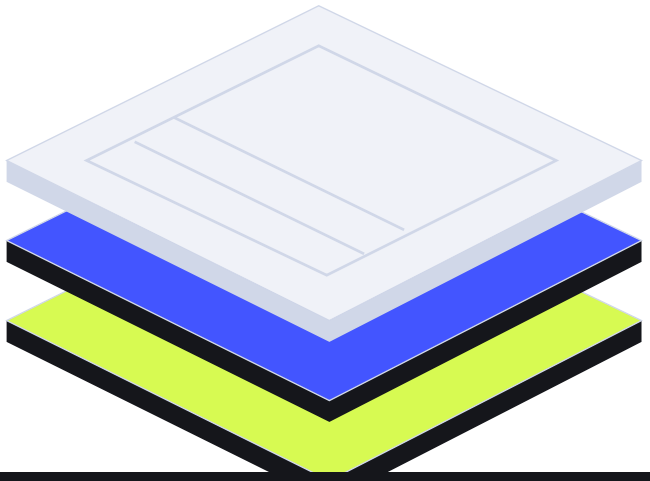
# What's beneath the build.

THE SHIPVRA REPORT

SAMPLE EDITION / NOT A CUSTOMER ASSESSMENT

A clear view of what stands between this application and production.

https://sample.shipvra.example/



SHIPVRA SCORE

85 / 100

OBSERVED PUBLIC APPLICATION

**Resolve critical findings before production release.**

8 FINDINGS / 1 CRITICAL

INSPECT > REPAIR > VERIFY > SHIP

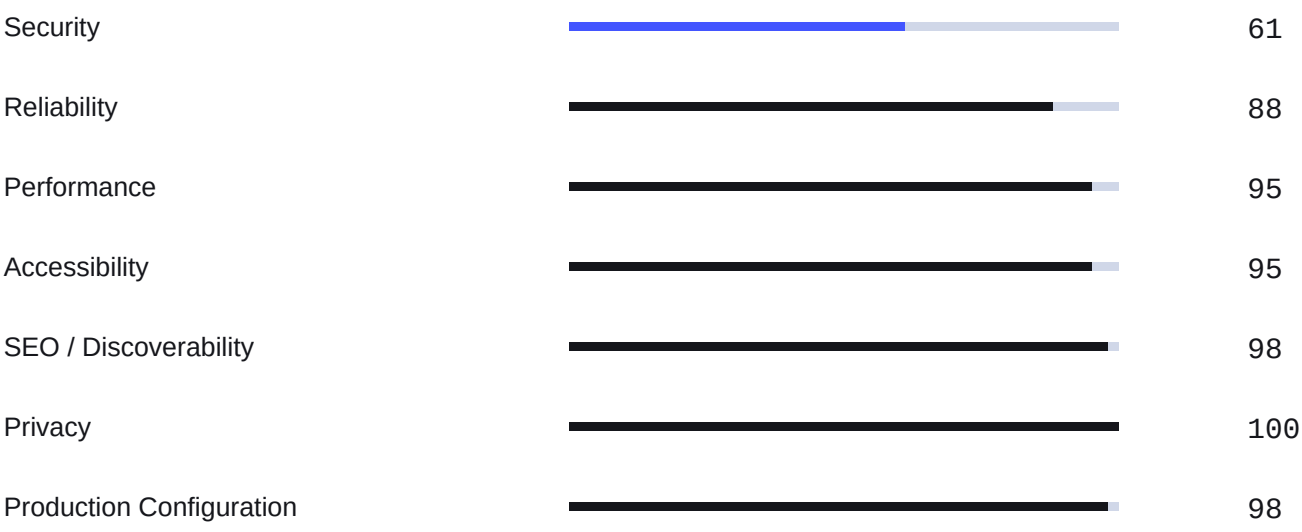
01 / EXECUTIVE DECISION

# The launch decision starts with evidence.

## Resolve critical findings before production release.

This is a point-in-time assessment of observable behavior. The score summarizes the checks performed; it does not establish that every production boundary was tested.

| 1 | 2 | 3 | 2 | 0 |
|---|---|---|---|---|
| CRITICAL | HIGH | MEDIUM | LOW | INFO |




| | |
|---|---|
| ASSESSMENT | COMPLETED |
| COMPLETED | 2026-09-12 / 14:30:00 UTC |
| SCANNER | shipvra-scanner/0.3.0 |
| SCAN ID | sample_scan_20260912 |

No deployment evidence record is included in this report. A high score does not remove the need to review signed-in workflows, payments, data permissions and operational recovery.

02 / REPAIR PRIORITIES

# Make the smallest correct change.

Start with the highest-risk findings. Preserve behavior, test the change and rerun the applicable check. A proposed repair is not a completed repair.

01 **A server credential is exposed in public configuration.**

FIX BEFORE LAUNCH / CRITICAL / Finding 01

Revoke and rotate the credential. Remove the file from the public deployment and repository history where applicable. Move required secrets to the server environment. Confirm the URL no longer returns configuration contents.

02 **A public route returns a server error.**

FIX BEFORE LAUNCH / HIGH / Finding 02

Trace the route in application logs using the assessment time. Repair the failing dependency or handler, add a regression check and confirm a successful deployed response.

03 **The session cookie is missing transport protections.**

FIX BEFORE LAUNCH / HIGH / Finding 03

Set Secure and HttpOnly server-side. Confirm intended SameSite behavior for authentication callbacks. Retest login, refresh and logout.

04 **No enforced Content Security Policy was observed.**

REVIEW BEFORE LAUNCH / MEDIUM / Finding 04

Inventory required origins. Introduce a policy using nonces or hashes where appropriate, then validate normal workflows before enforcement.

05 **The email field has no programmatic label.**

REVIEW BEFORE LAUNCH / MEDIUM / Finding 05

Add a visible label associated with the input ID. Verify the computed accessible name in the rendered application. Test keyboard submission and validation feedback.

06 **The initial document is unnecessarily large.**

REVIEW BEFORE LAUNCH / MEDIUM / Finding 06

Inspect repeated serialized data and embedded content. Remove avoidable payload, preserve cache behavior, then compare response size and separately measure the rendered experience.

07 **The homepage is missing its meta description.**

IMPROVEMENT / LOW / Finding 07

Write a precise description and include it in server-rendered metadata. Check that it is present in the deployed response.

08 **The response discloses its framework.**

IMPROVEMENT / LOW / Finding 08

Disable the response banner in the supported Next.js configuration. Validate the production build and rerun the deployed header check.

PLAN BOUNDARIES

Public findings are ordered by priority, severity and confidence. Priority is remediation guidance, not a verified launch blocker. Repository repair dependencies, when available, are recorded in Deep Inspect. This list does not infer dependencies from a public response.

03 / FINDING 01 OF 08

CRITICAL

# A server credential is exposed in public configuration.

FIX BEFORE LAUNCH / Security / Confidence: CONFIRMED

The public configuration response contains a variable matching a server credential pattern. The value is omitted from this report.

### WHY THIS MATTERS

A server credential may grant privileges that browser code should never hold. Treat confirmed exposure as a rotation event, not only a file removal.

### AFFECTED AREA

`https://sample.shipvra.example/.env`

### OBSERVED EVIDENCE

```
GET /.env -> HTTP 200
Pattern: server credential
Credential value: [OMITTED]
This observation is synthetic.
```

### RECOMMENDED REPAIR

Revoke and rotate the credential. Remove the file from the public deployment and repository history where applicable. Move required secrets to the server environment. Confirm the URL no longer returns configuration contents.

### FINDING PROVENANCE

`security/public-secret / v1`
`shipvra-scanner/0.3.0`
`Observed 2026-09-12 / 14:30:00 UTC`

03 / FINDING 02 OF 08

HIGH

# A public route returns a server error.

FIX BEFORE LAUNCH / Reliability / Confidence: CONFIRMED

A linked public route returned HTTP 500. This records a single response, not an uptime measurement.

### WHY THIS MATTERS

Customers following a visible link may be unable to complete their task. The response alone does not establish the cause.

### AFFECTED AREA

`https://sample.shipvra.example/pricing`

### OBSERVED EVIDENCE

```
GET /pricing -> HTTP 500
Content-Type: text/html
One bounded request observed
No repeated load applied
```

### RECOMMENDED REPAIR

Trace the route in application logs using the assessment time. Repair the failing dependency or handler, add a regression check and confirm a successful deployed response.

### FINDING PROVENANCE

`reliability/server-error / v1`
`shipvra-scanner/0.3.0`
`Observed 2026-09-12 / 14:30:00 UTC`

03 / FINDING 03 OF 08

HIGH

# The session cookie is missing transport protections.

FIX BEFORE LAUNCH / Security / Confidence: CONFIRMED

A session-like cookie is set without Secure and HttpOnly attributes. Cookie values are omitted.

### WHY THIS MATTERS

Secure restricts transport to HTTPS. HttpOnly reduces exposure to scripts. These controls support session confidentiality but do not replace secure session design.

### AFFECTED AREA

`https://sample.shipvra.example/`

### OBSERVED EVIDENCE

```
Cookie name: session
Secure: absent
HttpOnly: absent
SameSite: Lax
Cookie value: [OMITTED]
```

### RECOMMENDED REPAIR

Set Secure and HttpOnly server-side. Confirm intended SameSite behavior for authentication callbacks. Retest login, refresh and logout.

### FINDING PROVENANCE

`security/cookies / v1`
`shipvra-scanner/0.3.0`
`Observed 2026-09-12 / 14:30:00 UTC`

03 / FINDING 04 OF 08

MEDIUM

# No enforced Content Security Policy was observed.

REVIEW BEFORE LAUNCH / Security / Confidence: CONFIRMED

The root response has no enforcing Content-Security-Policy header. This identifies a missing defense, not confirmed script injection.

### WHY THIS MATTERS

A scoped policy limits which script sources execute. Test the policy against the application; a copied policy may break legitimate behavior.

### AFFECTED AREA

`https://sample.shipvra.example/`

### OBSERVED EVIDENCE

```
Content-Security-Policy: absent
Content-Security-Policy-Report-Only: absent
Response: HTTP 200
```

### RECOMMENDED REPAIR

Inventory required origins. Introduce a policy using nonces or hashes where appropriate, then validate normal workflows before enforcement.

### FINDING PROVENANCE

`security/csp-missing / v1`
`shipvra-scanner/0.3.0`
`Observed 2026-09-12 / 14:30:00 UTC`

03 / FINDING 05 OF 08

MEDIUM

# The email field has no programmatic label.

REVIEW BEFORE LAUNCH / Accessibility / Confidence: CONFIRMED

An email input has no associated label or accessible naming attribute in the observed HTML.

### WHY THIS MATTERS

Assistive technology needs an accessible name to communicate a control's purpose. Placeholder text is not a persistent label.

### AFFECTED AREA

`https://sample.shipvra.example/ / launch form`

### OBSERVED EVIDENCE

```
Element: input[type=email]
Associated label: not found
aria-label / aria-labelledby: absent
Detection: static HTML
```

### RECOMMENDED REPAIR

Add a visible label associated with the input ID. Verify the computed accessible name in the rendered application. Test keyboard submission and validation feedback.

### FINDING PROVENANCE

a11y/form-label / v1
shipvra-scanner/0.3.0
Observed 2026-09-12 / 14:30:00 UTC

03 / FINDING 06 OF 08

MEDIUM

# The initial document is unnecessarily large.

REVIEW BEFORE LAUNCH / Performance / Confidence: CONFIRMED

The document exceeds the configured payload threshold. This is a response-size observation, not a Core Web Vitals measurement.

### WHY THIS MATTERS

A large response increases transfer and parsing work, particularly on slower connections. Investigate the payload before selecting an optimization.

### AFFECTED AREA

`https://sample.shipvra.example/`

### OBSERVED EVIDENCE

```
Decoded document: 812 KB
Measured resource: root HTML
Core Web Vitals: not measured
Request location: scanner worker
```

### RECOMMENDED REPAIR

Inspect repeated serialized data and embedded content. Remove avoidable payload, preserve cache behavior, then compare response size and separately measure the rendered experience.

### FINDING PROVENANCE

`perf/large-document / v1`
`shipvra-scanner/0.3.0`
`Observed 2026-09-12 / 14:30:00 UTC`

03 / FINDING 07 OF 08

LOW

# The homepage is missing its meta description.

IMPROVEMENT / SEO / Confidence: CONFIRMED

No non-empty description metadata was found in the document head.

### WHY THIS MATTERS

A concise description communicates the page's purpose when a search engine chooses to use it. It does not guarantee appearance or ranking.

### AFFECTED AREA

`https://sample.shipvra.example/`

### OBSERVED EVIDENCE

```
Selector: meta[name=description]
Matching elements: 0
Page title: Launch your next product
```

### RECOMMENDED REPAIR

Write a precise description and include it in server-rendered metadata. Check that it is present in the deployed response.

### FINDING PROVENANCE

`seo/meta-description / v1`
`shipvra-scanner/0.3.0`
`Observed 2026-09-12 / 14:30:00 UTC`

03 / FINDING 08 OF 08

LOW

# The response discloses its framework.

IMPROVEMENT / Production Configuration / Confidence: CONFIRMED

A response header identifies the framework. Removing it reduces incidental disclosure; it does not prevent fingerprinting.

### WHY THIS MATTERS

Production responses should expose only necessary information. This is a narrow hardening change with a small expected scope.

### AFFECTED AREA

`https://sample.shipvra.example/`

### OBSERVED EVIDENCE

```
X-Powered-By: Next.js
Response: HTTP 200
Source configuration: not inspected
```

### RECOMMENDED REPAIR

Disable the response banner in the supported Next.js configuration. Validate the production build and rerun the deployed header check.

### FINDING PROVENANCE

`security/x-powered-by / v1`
`shipvra-scanner/0.3.0`
`Observed 2026-09-12 / 14:30:00 UTC`

04 / SOURCE AND REPAIR RECORD

# Follow the evidence into the codebase.

## Deep Inspect was not executed for this scan.

Authentication, authorization, database policies, payment correctness, dependencies, testing, CI/CD and observability are not verified by this public report. Connecting a repository enables separate source analysis.

### AUTOREPAIR AND PROOF RUN

No AutoRepair or source repair Proof Run was executed for this scan. No repair branch, commit or pull request is represented as completed.

### DEPLOYMENT EVIDENCE RECORD

Not issued. Source validation alone does not establish deployment verification. A deployment evidence record identifies the tested deployment, immutable commit, scanner version, timestamp and remaining findings.

05 / COVERAGE AND METHODOLOGY

# Know what was tested. Know what was not.

Completed means a rule executed, not that every possible defect in that category was ruled out. Missing or skipped checks remain visible.

SECURITY

| | |
|---|---|
| security/cookies / v1 | COMPLETED |
| security/csp-missing / v1 | COMPLETED |
| security/public-secret / v1 | COMPLETED |

RELIABILITY

| | |
|---|---|
| reliability/server-error / v1 | COMPLETED |

PERFORMANCE

| | |
|---|---|
| perf/large-document / v1 | COMPLETED |

ACCESSIBILITY

| | |
|---|---|
| a11y/form-label / v1 | COMPLETED |

SEO / DISCOVERABILITY

| | |
|---|---|
| seo/meta-description / v1 | COMPLETED |

PRIVACY

No recorded rule executions in this category.

PRODUCTION CONFIGURATION

| | |
|---|---|
| security/x-powered-by / v1 | COMPLETED |

DETERMINISTIC SCORING

Each public category begins at 100. A finding subtracts rounded(severity penalty x confidence multiplier x rule weight / 10), with a floor of zero. Severity penalties: Critical 22, High 12, Medium 5, Low 2, Info 0. Confidence multipliers: Confirmed 1.00, High 0.90, Medium 0.65, Low 0.35.

The rounded overall score weights Security 28%, Reliability 18%, Performance 14%, Accessibility 12%, SEO 10%, Privacy 8% and Production Configuration 10%. Incomplete scans withhold scores. Source findings are reported separately. No LLM assigns or adjusts scores.

## METHOD AND SAFETY BOUNDARIES

Non-destructive public observations use bounded GET requests. Network targets and redirects are validated, with connections pinned to the validated address. Evidence is sanitized. The assessment does not bypass authentication, brute-force credentials, alter customer data, create transactions or perform load testing.

## REMAINING MANUAL REVIEW

Review signed-in workflows, ownership and tenant isolation, payment entitlements, database policies, data integrity, keyboard operation, visual contrast, error recovery, monitoring, backups and deployment configuration. Static HTML observations do not execute the application. Browser behavior, Core Web Vitals and full accessibility conformance require separate measurement.

## INTERPRETATION AND LIMITATIONS

Results apply to the observed application at the time shown. Coverage is bounded and may miss conditional, authenticated or unvisited behavior. A confidence level expresses the strength of recorded evidence. An inference is not proof of exploitation. No findings is not the same as no defects. This report is neither a security certification nor proof of WCAG compliance.