# Gather Audit

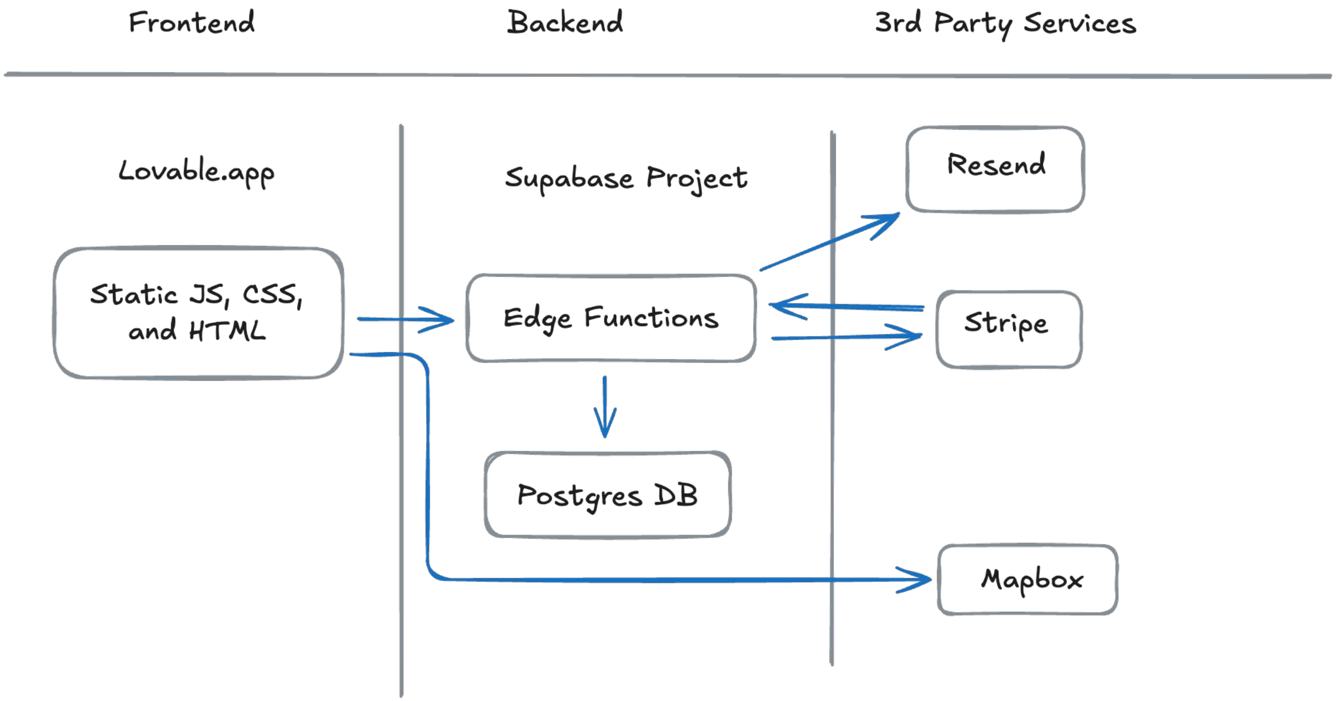
By: Erik Wiffin

# Summary

Application is in a good place, but **not** ready for production. Main issues are:

- lack of distinct production and development environments
- missing or non-functional test suite
- SEO bugs and necessary improvements

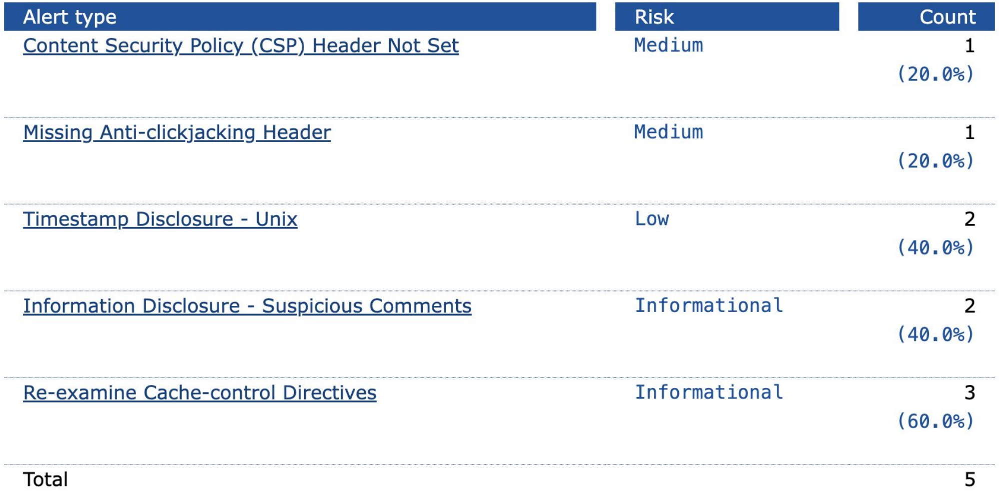
# Architecture



External Services:

- Supabase
- Stripe
- Resend
- Mapbox

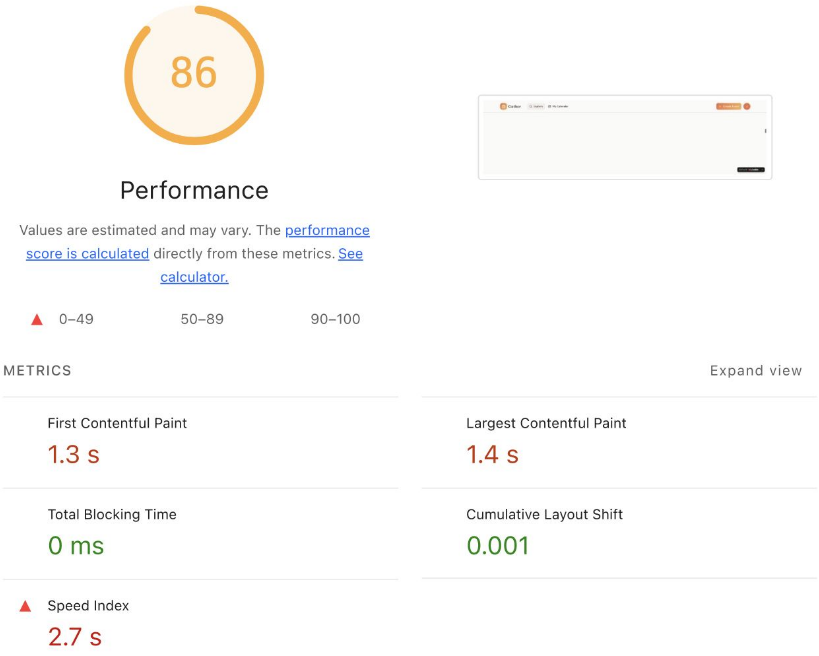
# ZAP by Checkmarx Scanning Report



| Alert type | Risk | Count |
|---|---|---|
| Content Security Policy (CSP) Header Not Set | Medium | 1 (20.0%) |
| Missing Anti-clickjacking Header | Medium | 1 (20.0%) |
| Timestamp Disclosure - Unix | Low | 2 (40.0%) |
| Information Disclosure - Suspicious Comments | Informational | 2 (40.0%) |
| Re-examine Cache-control Directives | Informational | 3 (60.0%) |
| Total | | 5 |

- Set recommended headers

# Performance Evaluation



86

Performance

Values are estimated and may vary. The performance score is calculated directly from these metrics. See calculator.

▲ 0–49 50–89 90–100

METRICS Expand view

First Contentful Paint
1.3 s

Largest Contentful Paint
1.4 s

Total Blocking Time
0 ms

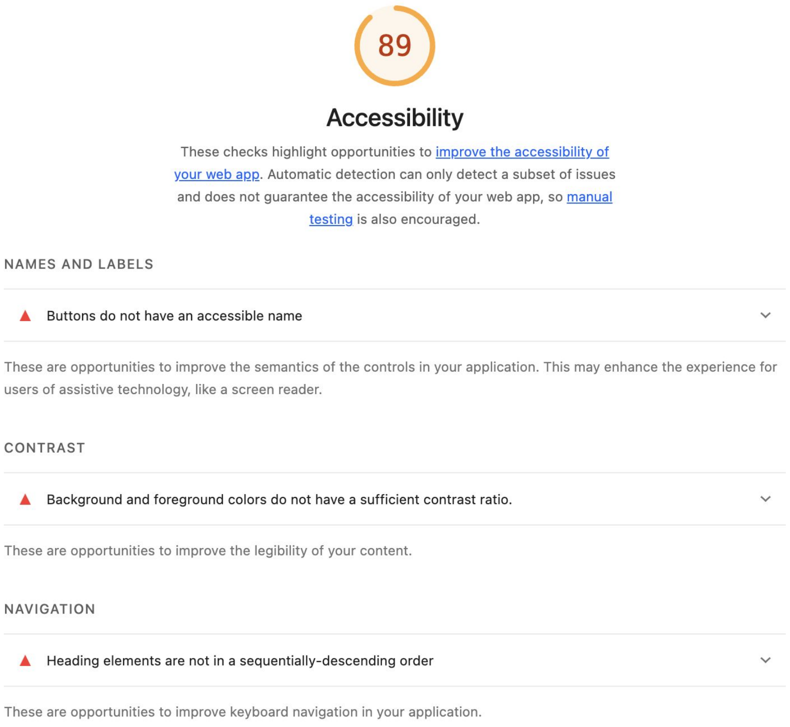
Cumulative Layout Shift
0.001

▲ Speed Index
2.7 s

- Paginate results + infinite scroll
- Geocoding is happening live, switch to geocoding at event creation time and cache results

# Accessibility - Lighthouse and Axe

- Fix recommended issues



89

## Accessibility

These checks highlight opportunities to improve the accessibility of your web app. Automatic detection can only detect a subset of issues and does not guarantee the accessibility of your web app, so manual testing is also encouraged.

NAMES AND LABELS

▲ Buttons do not have an accessible name

These are opportunities to improve the semantics of the controls in your application. This may enhance the experience for users of assistive technology, like a screen reader.

CONTRAST

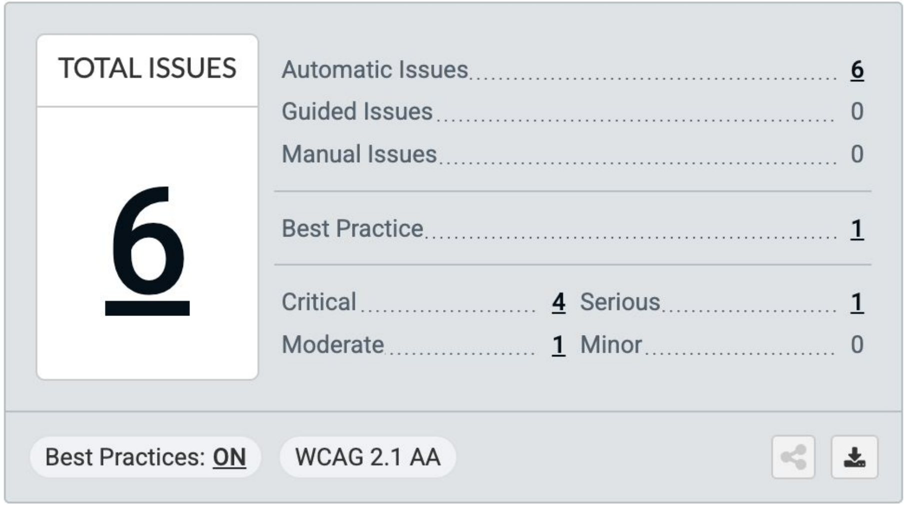
▲ Background and foreground colors do not have a sufficient contrast ratio.

These are opportunities to improve the legibility of your content.

NAVIGATION

▲ Heading elements are not in a sequentially-descending order

These are opportunities to improve keyboard navigation in your application.



TOTAL ISSUES

6

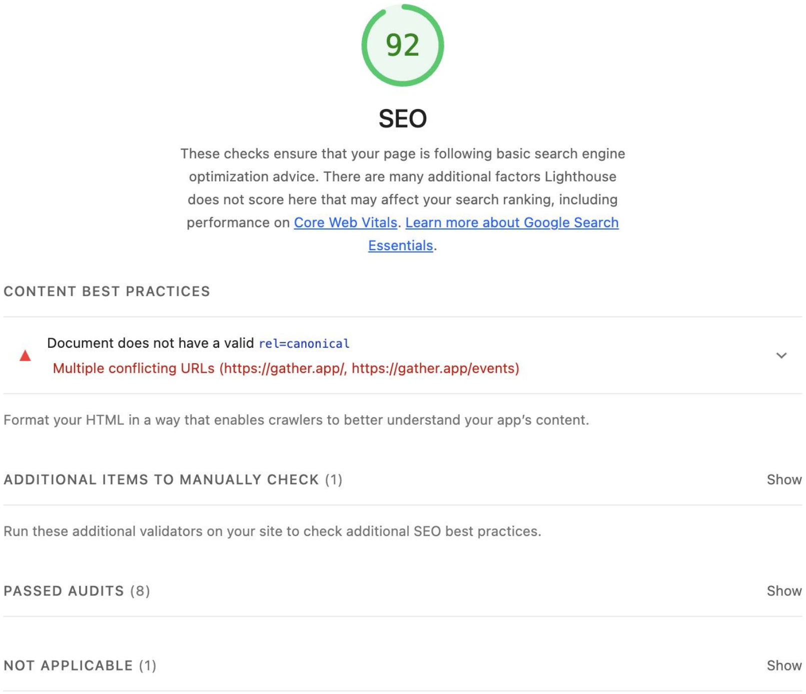
| | |
|---|---|
| Automatic Issues | 6 |
| Guided Issues | 0 |
| Manual Issues | 0 |
| Best Practice | 1 |

| | | | |
|---|---|---|---|
| Critical | 4 | Serious | 1 |
| Moderate | 1 | Minor | 0 |

Best Practices: ON

WCAG 2.1 AA

# SEO



92

SEO

These checks ensure that your page is following basic search engine optimization advice. There are many additional factors Lighthouse does not score here that may affect your search ranking, including performance on Core Web Vitals. Learn more about Google Search Essentials.

CONTENT BEST PRACTICES

▲ Document does not have a valid `rel=canonical`
Multiple conflicting URLs (https://gather.app/, https://gather.app/events)

Format your HTML in a way that enables crawlers to better understand your app's content.

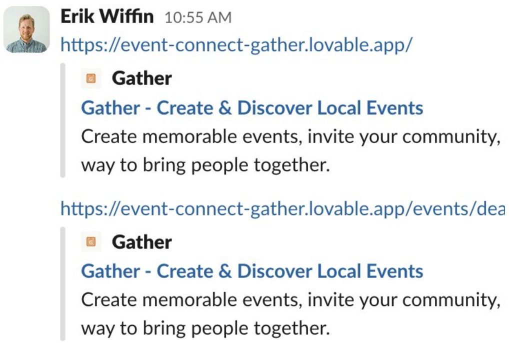
ADDITIONAL ITEMS TO MANUALLY CHECK (1) Show

Run these additional validators on your site to check additional SEO best practices.

PASSED AUDITS (8) Show

NOT APPLICABLE (1) Show

- Fix canonical URL
- Fix duplicate tags for social previews
- Sub-sitemaps, add events to sitemaps

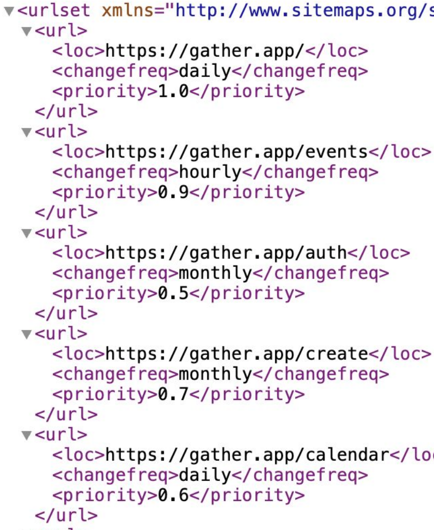


**Erik Wiffin** 10:55 AM
https://event-connect-gather.lovable.app/

**Gather**
Gather - Create & Discover Local Events
Create memorable events, invite your community, way to bring people together.

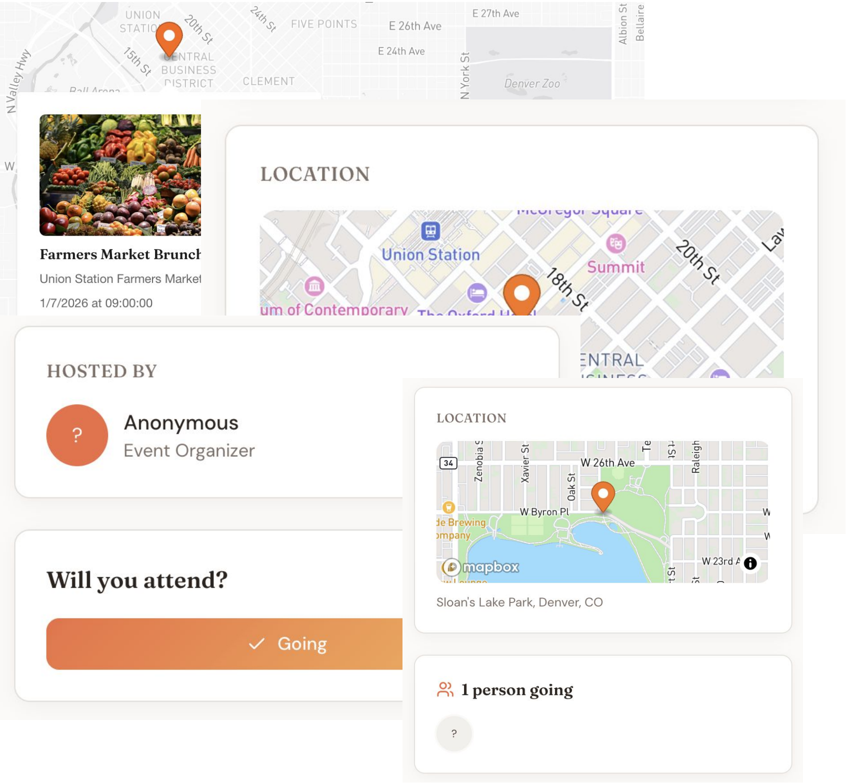
https://event-connect-gather.lovable.app/events/dea

**Gather**
Gather - Create & Discover Local Events
Create memorable events, invite your community, way to bring people together.



```
▼<urlset xmlns="http://www.sitemaps.org/s
  ▼<url>
     <loc>https://gather.app/</loc>
     <changefreq>daily</changefreq>
     <priority>1.0</priority>
   </url>
  ▼<url>
     <loc>https://gather.app/events</loc>
     <changefreq>hourly</changefreq>
     <priority>0.9</priority>
   </url>
  ▼<url>
     <loc>https://gather.app/auth</loc>
     <changefreq>monthly</changefreq>
     <priority>0.5</priority>
   </url>
  ▼<url>
     <loc>https://gather.app/create</loc>
     <changefreq>monthly</changefreq>
     <priority>0.7</priority>
   </url>
  ▼<url>
     <loc>https://gather.app/calendar</lo
     <changefreq>daily</changefreq>
     <priority>0.6</priority>
   </url>
```

# Design and Consistency



Farmers Market Brunch

Union Station Farmers Market

1/7/2026 at 09:00:00

LOCATION

HOSTED BY

?

Anonymous

Event Organizer

Will you attend?

✓ Going

LOCATION

Sloan's Lake Park, Denver, CO

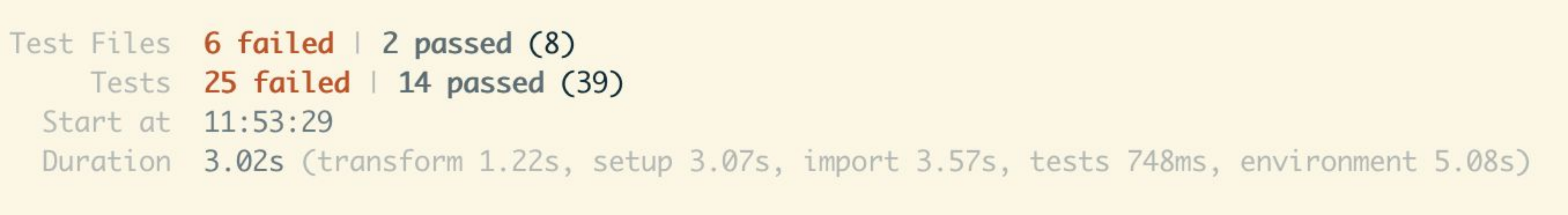
1 person going

?

- Use consistent map styles
- Update headers to be more consistent

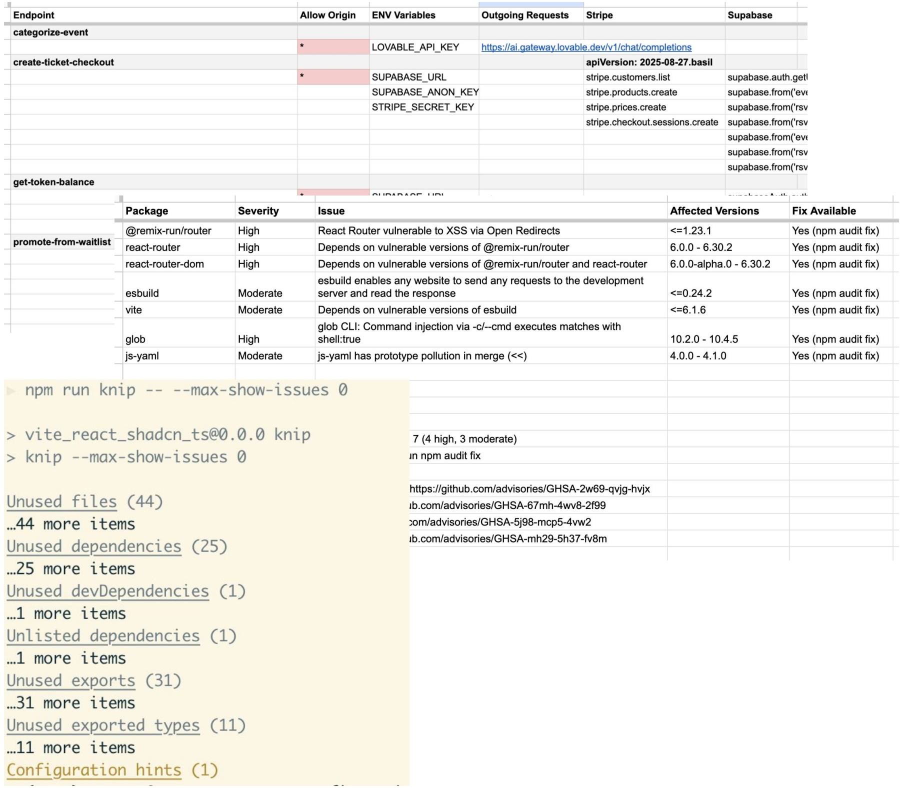
# Testing - Failure

- Add a comprehensive integration test suite for core user journeys
- Fix failing tests
- Integrate regression testing into software development workflow so that core user functionality does not degrade



```
Test Files  6 failed | 2 passed (8)
     Tests  25 failed | 14 passed (39)
  Start at  11:53:29
  Duration  3.02s (transform 1.22s, setup 3.07s, import 3.57s, tests 748ms, environment 5.08s)
```

# Code Quality



| Endpoint | Allow Origin | ENV Variables | Outgoing Requests | Stripe | Supabase |
|---|---|---|---|---|---|
| **categorize-event** | | | | | |
| | * | LOVABLE_API_KEY | https://ai.gateway.lovable.dev/v1/chat/completions | | |
| **create-ticket-checkout** | | | | **apiVersion: 2025-08-27.basil** | |
| | * | SUPABASE_URL | | stripe.customers.list | supabase.auth.get |
| | | SUPABASE_ANON_KEY | | stripe.products.create | supabase.from('eve |
| | | STRIPE_SECRET_KEY | | stripe.prices.create | supabase.from('rsv |
| | | | | stripe.checkout.sessions.create | supabase.from('rsv |
| | | | | | supabase.from('eve |
| | | | | | supabase.from('rsv |
| | | | | | supabase.from('rsv |
| **get-token-balance** | | | | | |
| | * | SUPABASE_URL | | | |
| **promote-from-waitlist** | | | | | |

| Package | Severity | Issue | Affected Versions | Fix Available |
|---|---|---|---|---|
| @remix-run/router | High | React Router vulnerable to XSS via Open Redirects | <=1.23.1 | Yes (npm audit fix) |
| react-router | High | Depends on vulnerable versions of @remix-run/router | 6.0.0 - 6.30.2 | Yes (npm audit fix) |
| react-router-dom | High | Depends on vulnerable versions of @remix-run/router and react-router | 6.0.0-alpha.0 - 6.30.2 | Yes (npm audit fix) |
| esbuild | Moderate | esbuild enables any website to send any requests to the development server and read the response | <=0.24.2 | Yes (npm audit fix) |
| vite | Moderate | Depends on vulnerable versions of esbuild | <=6.1.6 | Yes (npm audit fix) |
| glob | High | glob CLI: Command injection via -c/--cmd executes matches with shell:true | 10.2.0 - 10.4.5 | Yes (npm audit fix) |
| js-yaml | Moderate | js-yaml has prototype pollution in merge (<<) | 4.0.0 - 4.1.0 | Yes (npm audit fix) |

7 (4 high, 3 moderate)

ın npm audit fix

https://github.com/advisories/GHSA-2w69-qvjg-hvjx

ıb.com/advisories/GHSA-67mh-4wv8-2f99

com/advisories/GHSA-5j98-mcp5-4vw2

ıb.com/advisories/GHSA-mh29-5h37-fv8m

```
▶ npm run knip -- --max-show-issues 0

> vite_react_shadcn_ts@0.0.0 knip
> knip --max-show-issues 0

Unused files (44)
…44 more items
Unused dependencies (25)
…25 more items
Unused devDependencies (1)
…1 more items
Unlisted dependencies (1)
…1 more items
Unused exports (31)
…31 more items
Unused exported types (11)
…11 more items
Configuration hints (1)
```

- Distinct development, staging, and production environments
- Extract hard-coded LLM prompt
- Dynamic map default location
- Add CORS headers
- `npm audit fix`
- Remove unused code

# Next Steps

- The SEO bug definitely needs to get fixed, and a working set of integration tests to make sure we don’t break any of the functionality we currently have would go a long way to helping me sleep at night.
- Before exposing any of this to real users, I’d want to create a dedicated production environment with a database that is not connected to a coding agent. Luckily it was easy to export the app to Github and it wouldn't be a huge lift to get it deployed somewhere else.
- A few of the features need more work. The ticketed events feature doesn’t really do anything other than trigger a Stripe checkout flow. We’d probably want that to use Stripe Connect so event organizers could get paid, and give them more tools for managing purchased tickets and seeing their own revenue flow. The location autocomplete when creating an event could be better. Etc.
- No analytics have been configured beyond what Loveable comes with out of the box. A marketing team is going to know more than that, so they can see what kinds of events are attracting notice and how users are using the app.