Audit Report: Tallinn accommodation made easy - Larsen

Website: https://larsen.ee/
Date: 13.10.2026
Audit Coverage: 100% — all sources returned data
Confidence: medium

Pages Audited (5 of 5):

- https://larsen.ee/
- https://larsen.ee/about
- https://larsen.ee/faq
- https://larsen.ee/et/meist
- https://larsen.ee/corporate

Summary of results

Overall Score: 69 / 100
Status: **Needs Improvement**

Site overall 69 is the mean of 5 pages. Scores range 60 (https://larsen.ee/et/meist) → 76 (https://larsen.ee/). Weakest page: PSI mobile 68 vs desktop 88, with lab LCP 6.6 s and FCP 3.96 s on mobile — heavy penalties — though CrUX field data is fast (LCP 1068 ms p75, INP 96 ms, CLS 0). CLS 0.002 and TBT 0 ms are excellent, so the lab/field divergence is the main reason confidence is medium rather than high. Accessibility scores 91 but carries 2 axe violations, including a critical button-name on `.header__search-submit` and a serious color-contrast on the current-page nav link. Image assets are the biggest drag: 2.04 MB of images, 8/14 raster images without srcset, the hero lazy-loaded, and 8 images without explicit dimensions. Security basics FAILED (no HTTP→HTTPS redirect, no HSTS, no clickjacking protection, no CSP) and W3C reports 71 errors — both cap the overall below 90. SEO is missing a meta description and structured data.

Per-page scores

 Needs Improvement · https://larsen.ee/

Score	Performance	Accessibility	Best Practices	SEO	Security
76	91	91	81	85	FAILED

 Needs Improvement · https://larsen.ee/about

Score	Performance	Accessibility	Best Practices	SEO	Security
68	70	91	81	92	FAILED

 Needs Improvement · https://larsen.ee/faq

Score	Performance	Accessibility	Best Practices	SEO	Security
72	89	91	100	92	FAILED

 Needs Improvement · https://larsen.ee/et/meist

Score	Performance	Accessibility	Best Practices	SEO	Security
60	68	91	81	92	FAILED

 Needs Improvement · https://larsen.ee/corporate

Score	Performance	Accessibility	Best Practices	SEO	Security
67	71	91	81	85	FAILED

PageSpeed Insights — Mobile vs Desktop

*Lower is worse for Performance; higher is worse for LCP and CLS. Worse value is **bolded**.*

URL	Performance (M / D)	LCP (M / D)	CLS (M / D)
https://larsen.ee/	91 / **88**	**2.93 s** / 2.30 s	0.001 / **0.005**
https://larsen.ee/about	**70** / 88	**5.33 s** / 2.15 s	**0.004** / 0.001
https://larsen.ee/faq	**89** / 99	**3.02 s** / 795 ms	**0.029** / 0.000
https://larsen.ee/et/meist	**68** / 88	**6.63 s** / 2.15 s	**0.002** / 0.002
https://larsen.ee/corporate	**71** / 89	**6.85 s** / 2.11 s	0.001 / **0.006**

Optimization Checklist

4 of 7 passing — 4 pass · 0 warn · 3 fail · 1 n/a

Item	Status	Detail
Page caching plugin / CDN active	**Pass**	Caching plugin detected (WP Rocket) + CDN Cloudflare/Kinsta
Response compressed (gzip / brotli)	**Pass**	Document response is compressed with br.
Images lazy-loaded	**Pass**	All non-hero raster images use loading="lazy".
Hero image eagerly loaded	**Fail**	Hero image has loading="lazy", which delays LCP (inferred from DOM order/size — Lighthouse LCP element unavailable). Use loading="eager" (or omit loading) and add fetchpriority="high".
Hero is a real (not a CSS background-image)	N/A	No CSS background-images detected on raster-image-eligible elements.
Responsive images (srcset /)	**Fail**	11/17 raster images lack srcset and are not inside .
Reasonable number of image sizes	**Fail**	No raster images use srcset; browsers cannot pick an optimally sized variant.
JS scripts not blocking in	**Pass**	No render-blocking scripts in .

Fixes

Priority 1: Critical

Immediate action — impacts user experience, search rankings, or site safety.

1A. Load the hero image eagerly with high fetch priority `Performance`

- **Impact:** LCP
- **Problem:** The optimized-web checklist flags the hero image (menu-image-11.jpg) as loading="lazy" with no fetchpriority, and lab LCP is 2.9 s on mobile.
- **Solution:** Remove `loading="lazy"` from the hero `<img>` (or set `loading="eager"`) and add `fetchpriority="high"`:

  ```
  <img src=".../menu-image-11.jpg" alt="…" width="1200" height="800"
  fetchpriority="high">
  ```

  Keep `loading="lazy"` on all below-the-fold images.

1B. Cut image weight — convert and right-size `Performance`

- **Impact:** LCP, page weight, Speed Index
- **Problem:** PSI's image-delivery-insight estimates 251 KiB of savings, and the browser runtime shows 2.92 MB of images across 23 requests (out of 3.24 MB total).
- **Solution:**
  - Serve WebP/AVIF with a `<picture>` fallback.
  - Right-size: the runtime shows 800×800 and 1008×630 JPEGs at 99–145 KB each.
  - Extend `srcset` / `sizes` to the remaining 11 images (currently 29/40).
  - Re-encode the 225 KB `inter-tight-variable.woff2` and subset the font.

1C. Give the search submit button an accessible name `Accessibility`

- **Impact:** WCAG 4.1.2 (button-name)
- **Problem:** axe reports a critical `button-name` violation on `.header__search-submit` — the button has no discernible text.
- **Solution:** Add a visible label or an `aria-label`:

  ```
  <button class="header__search-submit" aria-label="Search">…
  </button>
  ```

1D. Load the hero image eagerly with fetchpriority="high" `Performance`

- **Impact:** LCP, FCP, Speed Index
- **Problem:** The Optimized-Web checklist flags the hero image (menu-image-11.jpg) as loading="lazy" with no fetchpriority, and mobile lab LCP is 5.3 s / FCP 4.08 s.
- **Solution:** Mark the hero as the highest-priority resource:

```
<img src="/wp-content/uploads/2026/05/menu-image-11.jpg"
     alt="…" width="1600" height="900"
     loading="eager" fetchpriority="high" decoding="async">
```

Also add a `<link rel="preload" as="image" fetchpriority="high" href="…">` in `<head>` so the browser starts the fetch before the parser reaches the tag.

1E. Cut image payload: add srcset and serve WebP/AVIF `Performance`

- **Impact:** LCP, page weight, Speed Index
- **Problem:** Browser runtime shows 1.65 MB of images out of 1.97 MB total; 11/17 raster images lack srcset and are not inside `<picture>`, and PSI's image-delivery-insight estimates 363 KiB of savings.
- **Solution:**
  - Add `srcset` + `sizes` to every raster image (WP Rocket / WordPress can emit these automatically).
  - Encode WebP/AVIF with a raster fallback:

```
<picture>
  <source type="image/webp" srcset="hero-800.webp 800w, hero-
1600.webp 1600w" sizes="100vw">
  <img src="hero-800.jpg" alt="…" width="1600" height="900">
</picture>
```

  - Re-encode the 800×800 property thumbnails and 560×1120 hero JPEGs, which dominate the byte count.

1F. Redirect HTTP to HTTPS and enable HSTS `Security`

- **Impact:** Transport security, MITM protection
- **Problem:** Security basics reports 'Plain HTTP does not redirect to HTTPS' and 'Strict-Transport-Security header is missing' — both basic-tier failures.
- **Solution:** Add a permanent redirect at the edge/origin and send HSTS:

```
# nginx
server { listen 80; server_name larsen.ee; return 301
https://$host$request_uri; }

# response header
Strict-Transport-Security: max-age=63072000; includeSubDomains;
preload
```

Verify preload eligibility at hstspreload.org before submitting.

1G. Add a meta description `SEO`

- **Impact:** SERP snippet, CTR
- **Problem:** PSI's `meta-description` audit scores 0 and the HTML inventory shows `Description: not set`.
- **Solution:** Add a unique 120–160 character description to the page head:

```
<meta name="description" content="Fully furnished rooms in Tartu
and Tallinn — book a viewing or contact Larsen's accommodation
adviser.">
```

1H. Redirect HTTP to HTTPS and add HSTS `Security`

- **Impact:** Transport security, MITM exposure
- **Problem:** Security basics reports 'Plain HTTP does not redirect to HTTPS' and 'Strict-Transport-Security header is missing' — both basic-tier fails.
- **Solution:**
  - At the edge (Cloudflare) enable 'Always Use HTTPS' and add an origin rule redirecting `http://larsen.ee/*` → `https://larsen.ee/$1`.
  - Send HSTS from the origin:

```
Header always set Strict-Transport-Security "max-age=63072000;
includeSubDomains; preload"
```

  - Submit to hstspreload.org once stable.

1I. Eager-load the hero image and set fetchpriority `Performance`

- **Impact:** LCP, FCP
- **Problem:** The optimized-web checklist flags the hero (`menu-image-11.jpg`) as `loading="lazy"` with no `fetchpriority`, delaying LCP (mobile LCP 3.0 s).
- **Solution:**

```
<img src="…/menu-image-11.jpg" alt="…" width="1200" height="800"
     loading="eager" fetchpriority="high" decoding="async">
```

  Keep `loading="lazy"` on below-the-fold images only.

1J. Force HTTP→HTTPS redirect `Security`

- **Impact:** Transport security, HSTS eligibility
- **Problem:** Security basics reports 'Plain HTTP does not redirect to HTTPS' — a basic-tier FAILED check.

- **Solution:** Add a 301 redirect at the edge/origin:

```
RewriteEngine On
RewriteCond %{HTTPS} off
RewriteRule ^ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]
```

  Or in Cloudflare: enable 'Always Use HTTPS'.

1K. Load the hero image eagerly with high fetchpriority `Performance`

- **Impact:** LCP, FCP
- **Problem:** Optimized-Web checklist flags the hero (`menu-image-11.jpg`) as `loading="lazy"` with no `fetchpriority` , which delays LCP (lab 6.6 s mobile).
- **Solution:**

```
<img src="/wp-content/uploads/2026/05/menu-image-11.jpg"
     alt="…" width="1600" height="900"
     loading="eager" fetchpriority="high" decoding="async">
```

1L. Cut LCP via image delivery and document latency `Performance`

- **Impact:** LCP, FCP, Speed Index
- **Problem:** PSI mobile LCP is 6.6 s with `image-delivery-insight` (363 KiB savings) and `document-latency-insight` (430 ms savings) as the top contributors.
- **Solution:**
  - Serve WebP/AVIF variants of the 2.04 MB of JPEGs.
  - Preload the LCP image: `<link rel="preload" as="image" href="…" fetchpriority="high">` .
  - Reduce TTFB (field p75 890 ms) by warming the Kinsta/Cloudflare cache and trimming server-side work.

1M. Cut image weight — 764 KiB of savings available `Performance`

- **Impact:** LCP, page weight, mobile performance
- **Problem:** PSI image-delivery-insight estimates 764 KiB of savings; browser runtime shows 19 images at 2.45 MB out of 2.76 MB total, and the sampled inventory is entirely .jpg/.jpeg/.png.
- **Solution:**
  - Serve WebP/AVIF with a `<picture>` fallback:

```
<picture>
  <source type="image/webp" srcset="hero-800.webp 800w, hero-
```

```
1600.webp 1600w" sizes="100vw">
  <img src="hero-800.jpg" alt="…" width="1600" height="900">
</picture>
```

- Right-size the 800×800 and 400×400 JPEGs currently being downloaded (e.g. larsen-st-38031-800x800.jpg at 120.8 KB, ttun5635-1-800x800.jpg at 104.5 KB).
- Enable WebP conversion in WP Rocket / Imagify and re-upload existing uploads.

1N. Give the header search button an accessible name `Accessibility`

- **Impact:** WCAG 2.1.1 / 4.1.2, screen-reader usability
- **Problem:** axe reports a critical `button-name` violation on `.header__search-submit` — the button has no discernible text.
- **Solution:**
  - Add visible text or an `aria-label`:

```
<button class="header__search-submit" type="submit" aria-
label="Search">
  <svg aria-hidden="true" focusable="false">…</svg>
</button>
```

  - If the icon is decorative, keep `aria-hidden="true"` on the SVG so the label is the only accessible name.

Priority 2: Important

Essential for compliance, user reach, and search visibility.

2A. Fix color contrast on the current nav link `Accessibility`

- **Impact:** WCAG 1.4.3 (color-contrast)
- **Problem:** axe reports a serious `color-contrast` violation on `.is-current[aria-current="page"]`; 15 additional nodes were flagged as incomplete.
- **Solution:** Raise the foreground/background contrast to ≥4.5:1 for the active nav state, then re-run axe to clear the 15 incomplete nodes.

2B. Add HSTS and clickjacking protection `Security`

- **Impact:** Transport security, clickjacking
- **Problem:** Security basics is FAILED: Strict-Transport-Security is missing and neither X-Frame-Options nor CSP frame-ancestors is set.
- **Solution:** Send from origin (Apache shown):

```
Header always set Strict-Transport-Security "max-age=63072000;
includeSubDomains; preload"
Header always set X-Frame-Options "SAMEORIGIN"
```

Or use `Content-Security-Policy: frame-ancestors 'self'`.

2C. Add a meta description `SEO`

- **Impact:** SERP snippet, CTR
- **Problem:** HTML inventory shows `Description: not set` and PSI's SEO score is 85 with `meta-description` failing.
- **Solution:** Add a unique 120–160 character description:

```
<meta name="description" content="Furnished co-living and short-
stay apartments across Tallinn — instant booking, flexible stays.">
```

2D. Fix srcset/sizes and inline style errors `Best Practices`

- **Impact:** HTML validity, responsive images
- **Problem:** W3C reports 78 errors; the top group is 'srcset with width descriptor requires sizes' ×12, plus 4 script `defer` on data-block types and many inline `@scope` style-rule errors.
- **Solution:**
  - Add `sizes` to every `<img>` that uses width descriptors in `srcset`.
  - Move the inline `<style id="larsen-book-a-tour-styles">` block out of `<body>` or wrap its rules in `@scope`.
  - Remove `defer` from `<script type="text/rocketlazyloadscript">` data blocks.

2E. Add explicit width/height to 11 images `Performance`

- **Impact:** CLS
- **Problem:** HTML inventory shows 11 of 40 images without explicit width/height, which can cause layout shifts.
- **Solution:** Add `width` and `height` attributes matching the intrinsic aspect ratio to every `<img>` (CSS `aspect-ratio` also works).

2F. Label the two unlabeled text inputs `Accessibility`

- **Impact:** WCAG 3.3.2, 4.1.2
- **Problem:** HTML inventory shows Form 2 with two text inputs marked 'no label'.
- **Solution:** Associate each input with a `<label for>` or add `aria-label`:

```
<label for="checkin">Check-in</label>
<input id="checkin" type="text">
```

2G. Add clickjacking protection `Security`

- **Impact:** Clickjacking, UI redressing
- **Problem:** Security basics reports 'Neither X-Frame-Options nor CSP frame-ancestors is set — the page can be framed'.
- **Solution:** Prefer CSP frame-ancestors; keep X-Frame-Options as a legacy fallback:

```
Content-Security-Policy: frame-ancestors 'self';
X-Frame-Options: SAMEORIGIN
```

2H. Fix contrast on the current-page nav link `Accessibility`

- **Impact:** WCAG 1.4.3, readability
- **Problem:** axe reports a serious `color-contrast` violation on `.is-current[aria-current="page"][href$="about/"]`.
- **Solution:** Darken the active-link color to reach ≥4.5:1 against its background (or ≥3:1 if it qualifies as large text). Also review the 6 'incomplete' contrast nodes axe could not evaluate (gradients / alpha).

2I. Fix the 72 W3C HTML errors `Best Practices`

- **Impact:** HTML validity, SEO, robustness
- **Problem:** W3C reports 72 errors including 6× `Attribute "src" not allowed on element "source"`, an `area-hidden` typo on the search form, an empty `href` on a dns-prefetch link, and `defer` / `async` on `text/rocketlazyloadscript` data blocks.
- **Solution:**
  - Replace `<source src="…">` with `<source srcset="…">` (or use `<img>` directly).
  - Fix the typo: `area-hidden="true"` → `aria-hidden="true"` on `<form id="header-search">`.
  - Remove the empty `href=""` from the dns-prefetch `<link>`.
  - Drop `defer` / `async` from `<script type="text/rocketlazyloadscript">` data blocks.
  - Move the inline `<style id="larsen-book-a-tour-styles">` out of `<body>` or wrap its rules in `@scope`.

2J. Investigate the 3 aborted image requests `Performance`

- **Impact:** LCP, image rendering
- **Problem:** Browser runtime captured 3 `net::ERR_ABORTED` image requests (11-4-820x1640.jpg, 2-3-820x1640.jpg, 5.jpg) — likely a srcset/lazy-load race.
- **Solution:**
  - Confirm the 820×1640 variants exist on disk and are not 404s.
  - Check that `sizes` matches the rendered layout so the browser does not pick a candidate it then aborts.
  - Ensure lazy-loaded images are not swapped by JS after the browser has already started the fetch.

2K. Emit valid structured data `SEO`

- **Impact:** Rich results, entity understanding
- **Problem:** PSI's `structuredData` audit fails and the single JSON-LD block is typed 'Unknown'.
- **Solution:** Add a proper `@type` (e.g. `Organization`, `LocalBusiness`, `RealEstateAgent`) with `name`, `url`, `logo`, and `address`, and validate with Google's Rich Results Test.

2L. Harden the WordPress install surface `Security`

- **Impact:** Attack surface, takeover risk
- **Problem:** Security basics flags `readme.html` as public, `/wp-admin/install.php` as reachable, and the login form served on the default `/wp-login.php` path.
- **Solution:**

```
# Block readme and installer
<Files "readme.html">
  Require all denied
</Files>
<Files "install.php">
  Require all denied
</Files>
```

  - Rename or protect the login path (e.g. a WAF rule or a plugin that moves `/wp-login.php`).
  - Add rate limiting / 2FA on the login endpoint.

2M. Fix color contrast on current-page links `Accessibility`

- **Impact:** WCAG 1.4.3 (Contrast)

- **Problem:** axe reports a serious `color-contrast` violation on `.is-current[aria-current="page"]` in the header and footer navigation.
- **Solution:** Raise the current-page link color to ≥4.5:1 against its background (or ≥3:1 if ≥18.66 px bold / 24 px). Verify with DevTools' contrast checker.

2N. Fix invalid aria-expanded="" on 53 buttons `Accessibility`

- **Impact:** WCAG 4.1.2, screen-reader state
- **Problem:** W3C reports 53 errors of 'Bad value "" for attribute "aria-expanded" on element "button"' — an empty string is not a valid ARIA boolean.
- **Solution:** Set `aria-expanded` to `"true"` or `"false"` (or remove it when the button doesn't control an expandable region):

  ```
  <button aria-expanded="false" aria-controls="…">…</button>
  ```

  Also fix the related `area-hidden="true"` typo on `#header-search` (should be `aria-hidden`).

2O. Serve responsive images (srcset /) and WebP `Performance`

- **Impact:** LCP, page weight, image bytes
- **Problem:** 11/11 raster images lack srcset and are not inside `<picture>`; 0 WebP. Images total 919 KB of the 1.21 MB page.
- **Solution:** Generate multiple sizes and modern formats:

  ```
  <picture>
    <source type="image/webp" srcset="hero-800.webp 800w, hero-
  1600.webp 1600w" sizes="100vw">
    <img src="hero-1600.jpg" srcset="hero-800.jpg 800w, hero-1600.jpg
  1600w" sizes="100vw" alt="…" width="1600" height="900">
  </picture>
  ```

  WP Rocket / a WebP plugin can automate this for WordPress uploads.

2P. Add explicit width/height to all images `Performance`

- **Impact:** CLS
- **Problem:** HTML inventory reports 11 images without explicit width/height; the layout-shift source is `main#main > div.h-container > div.grid > div.grid__col`.
- **Solution:** Add intrinsic dimensions to every `<img>` (and matching CSS `aspect-ratio` where the image is fluid) so the browser can reserve space before load.

2Q. Add HSTS `Security`

- **Impact:** Transport security, downgrade protection
- **Problem:** `strict-transport-security` is missing (basic-tier FAILED).
- **Solution:**

  ```
  Strict-Transport-Security: max-age=63072000; includeSubDomains;
  preload
  ```

  Submit to hstspreload.org once stable.

2R. Add srcset to the 8 images that lack it `Performance`

- **Impact:** Image bytes, LCP
- **Problem:** 8/14 raster images lack `srcset` and are not inside `<picture>`; total image bytes are 2.04 MB.
- **Solution:** Generate responsive variants (WP Rocket / Kinsta image optimization) and emit `srcset` + `sizes` for each content image.

2S. Fix color contrast on the current-page nav link `Accessibility`

- **Impact:** WCAG 1.4.3
- **Problem:** axe reports a serious `color-contrast` violation on `.is-current[aria-current="page"][href$="meist/"]`; 6 more nodes are 'incomplete'.
- **Solution:** Raise the active-link color to ≥4.5:1 against its background, and re-check the 6 incomplete nodes (alpha/gradient backgrounds).

2T. Fix the 71 W3C HTML errors `Best Practices`

- **Impact:** Markup validity, parser robustness
- **Problem:** W3C reports 71 errors, including 6× `src` not allowed on `<source>`, 4× `defer` on a data-block `<script>`, and dozens of style rules outside `@scope`.
- **Solution:**
  - Remove `src` from `<source>` elements (use `srcset` only).
  - Drop `defer` / `async` from `<script type="text/rocketlazyloadscript">`.
  - Move the inline `<style id="larsen-book-a-tour-styles">` block into `<head>` or wrap rules in `@scope`.

2U. Add explicit width/height to 8 images `Performance`

- **Impact:** CLS
- **Problem:** HTML inventory shows 8 images without `width` / `height`; CLS is currently 0.002 but the risk is latent.

- **Solution:** Set intrinsic `width` / `height` on every `<img>` (or use `aspect-ratio` in CSS) so the browser reserves space before load.

2V. Fix contrast on the mailto and tel links `Accessibility`

- **Impact:** WCAG 1.4.3 contrast
- **Problem:** axe reports a serious `color-contrast` violation on `a[href$="mailto:karl@larsen.ee"]` and `a[href="tel:+37253535858"]`; 6 further nodes were flagged as incomplete.
- **Solution:**
  - Darken the link color (or its background) to reach ≥4.5:1 for body text.
  - Re-check the 6 'incomplete' nodes manually — axe skips elements with gradients or alpha transparency.

2W. Make the carousel keyboard-scrollable `Accessibility`

- **Impact:** WCAG 2.1.1 / 2.1.3 keyboard access
- **Problem:** axe reports a serious `scrollable-region-focusable` violation on `.carousel-block__slider` — the scrollable region cannot be reached by keyboard.
- **Solution:**
  - Add `tabindex="0"` and a role/label to the scroll container:

```
<div class="carousel-block__slider" tabindex="0" role="region"
aria-label="Property carousel">
```

  - Ensure a visible focus ring and that arrow keys scroll the region.

2X. Replace vague repeated link text `SEO`

- **Impact:** Link context, SEO score
- **Problem:** PSI flags `link-text` (6 links) and the inventory shows "learn more" repeated 6 times, plus "home", "locations", "features" and "testimonials" three times each.
- **Solution:**
  - Make each link's text describe its destination, e.g. "Learn more about flexible terms" instead of "learn more".
  - Where the visible text must stay short, disambiguate with `aria-label`:

```
<a href="/apartments/sume/" aria-label="Learn more about Sume
House">Learn more</a>
```

2Y. Add width/height to the 11 unsized images `Performance`

- **Impact:** CLS, layout stability
- **Problem:** HTML inventory reports 11 of 43 images without explicit width/height, which the checklist flags as a layout-shift risk.
- **Solution:**
  - Add intrinsic `width` / `height` attributes (or an `aspect-ratio` in CSS) to every raster `<img>` so the browser can reserve space before load.
  - Keep the existing `srcset` / `sizes` pairs in sync with the declared dimensions.

2Z. Fix the 67 W3C validation errors `Best Practices`

- **Impact:** Markup correctness, cross-browser rendering
- **Problem:** W3C reports 67 errors and 7 warnings; the largest group is a plugin injecting `<style>` blocks with `@scope` rules into `<body>` (`.lbt-*` classes), plus a duplicate ID `section-1778511488647-5` , `src` on `<source>` (×3), and an `area-hidden` typo on the search form.
- **Solution:**
  - Fix the typo first — it silently disables the intended attribute:

```
<form id="header-search" class="header__search-form" aria-
hidden="true" role="search">
```

  - Move the plugin's `<style id="larsen-book-a-tour-styles">` block into `<head>` (or scope it correctly) instead of emitting it mid- `<body>` .
  - Remove `src` from `<source>` elements that only carry `srcset` .
  - De-duplicate the `section-1778511488647-5` ID.

2[. Close WordPress hygiene gaps `Security`

- **Impact:** Attack surface, information disclosure
- **Problem:** Security basics reports readme.html is public, /wp-admin/install.php is reachable, and the login form is served on the default /wp-login.php path.
- **Solution:**
  - Block the readme and installer:

```
<Files "readme.html">
  Require all denied
</Files>
<Files "install.php">
  Require all denied
</Files>
```

- Move or rename the login path (e.g. a custom login slug) and rate-limit `/wp-login.php`.
- Keep xmlrpc.php blocked (already passing).

2. Add SRI to the two cross-origin scripts `Security`

- **Impact:** Supply-chain integrity
- **Problem:** Security basics reports 2 of 2 cross-origin scripts lack an `integrity` attribute; both are loaded from cdn.jsdelivr.net (iframemanager, cookieconsent).
- **Solution:**
  - Pin versions and add hashes:

```
<script
src="https://cdn.jsdelivr.net/gh/orestbida/cookieconsent@3.0.1/dist
/cookieconsent.umd.js"
        integrity="sha384-…" crossorigin="anonymous" defer>
</script>
```

  - Better still, self-host these two libraries so they fall under your own CSP.

Priority 3: Best Practice

Recommended for long-term maintainability.

3A. Disambiguate repeated vague link text `SEO`

- **Impact:** Link purpose, SEO
- **Problem:** HTML inventory shows 'learn more' ×6 and PSI's `link-text` audit fails with 6 links.
- **Solution:** Rewrite anchor text to describe the destination (e.g. 'Learn more about Sume') or add `aria-label`.

3B. Harden WordPress exposure paths `Security`

- **Impact:** Attack surface
- **Problem:** Security basics flags readme.html as public, /wp-admin/install.php as reachable, and login served on the default /wp-login.php path.
- **Solution:**
  - Delete or block `readme.html`.
  - Block `/wp-admin/install.php` in `.htaccess`.
  - Move or rate-limit the login path (e.g. a custom login URL plugin + WAF rule).

3C. Add a nonce-based CSP if the site later gains auth or user content `Security`

- **Impact:** XSS defense-in-depth (low value today)
- **Problem:** CSP is missing, but site signals show no auth, payments, user-generated content, or e-commerce, so XSS attack surface is minimal — listed as P3 per the rubric.
- **Solution:** If/when you add login or user content, deploy a nonce-based CSP rather than a flat allowlist:

  ```
  Content-Security-Policy: script-src 'nonce-{random}' 'strict-dynamic'; object-src 'none'; base-uri 'none';
  ```

  For the current brochure site, prioritize the P1/P2 items above.

3D. Add explicit width/height to the 11 dimension-less images `Performance`

- **Impact:** CLS (latent)
- **Problem:** HTML inventory shows 11 of 17 images without explicit width/height; current CLS is 0.004 so the risk is latent rather than active.
- **Solution:** Add intrinsic `width` / `height` attributes or a CSS `aspect-ratio` so the browser can reserve space before the image loads.

3E. Add a nonce-based CSP `Security`

- **Impact:** XSS defense-in-depth
- **Problem:** CSP is missing. Site signals show no auth, payments, user content, or e-commerce, so the XSS attack surface is limited — P3 per the rubric, not P1.
- **Solution:** If you later add login or user content, deploy a nonce + `'strict-dynamic'` policy rather than a flat allowlist:

  ```
  Content-Security-Policy: script-src 'nonce-{random}' 'strict-dynamic'; object-src 'none'; base-uri 'none';
  ```

3F. Add Referrer-Policy, Permissions-Policy, COOP, CORP, and SRI `Security`

- **Impact:** Privacy, origin isolation, supply-chain integrity
- **Problem:** Referrer-Policy, Permissions-Policy, Cross-Origin-Opener-Policy, and Cross-Origin-Resource-Policy are all missing, and 2/2 cross-origin scripts lack an `integrity` attribute.
- **Solution:**

  ```
  Referrer-Policy: strict-origin-when-cross-origin
  Permissions-Policy: camera=(), microphone=(), geolocation=()
  Cross-Origin-Opener-Policy: same-origin
  Cross-Origin-Resource-Policy: same-origin
  ```

Add `integrity="sha384-…"` + `crossorigin="anonymous"` to the jsdelivr scripts (iframemanager, cookieconsent).

3G. Resolve the deprecated-API warning `Best Practices`

- **Impact:** Future browser compatibility
- **Problem:** PSI's `deprecations` audit scores 0 with 1 warning found.
- **Solution:** Open the Lighthouse deprecations audit in the report to identify the specific API, then replace it with its modern equivalent (commonly `document.write`, `XMLHttpRequest` sync, or `unload` handlers).

3H. Enlarge tap targets `SEO`

- **Impact:** Mobile usability
- **Problem:** PSI's `tapTargets` audit fails on mobile.
- **Solution:** Ensure every interactive element is at least 48×48 px with adequate spacing (WCAG 2.5.8).

3I. Raise the browser cache TTL `Performance`

- **Impact:** Repeat-visit performance
- **Problem:** `cache-control: public, max-age=0, s-maxage=86400` disables browser caching — only the edge caches for 24 h.
- **Solution:** Set a long `max-age` on hashed static assets (JS/CSS/fonts) while keeping HTML short-lived:

```
Cache-Control: public, max-age=31536000, immutable
```

3J. Add a nonce-based Content-Security-Policy `Security`

- **Impact:** XSS defense-in-depth
- **Problem:** CSP is missing. Site signals show no auth, payments, or user-generated content, so XSS attack surface is minimal — listed as P3 per the rubric.
- **Solution:** Deploy a nonce + `'strict-dynamic'` CSP rather than a flat allowlist:

```
Content-Security-Policy: default-src 'self'; script-src 'nonce-
{random}' 'strict-dynamic'; object-src 'none'; base-uri 'none';
```

3K. Add Referrer-Policy, Permissions-Policy, COOP and CORP `Security`

- **Impact:** Privacy, origin isolation
- **Problem:** All four headers are missing per the security-headers scan.
- **Solution:**

```
Header always set Referrer-Policy "strict-origin-when-cross-origin"
Header always set Permissions-Policy "geolocation=(), microphone=
(), camera=()"
Header always set Cross-Origin-Opener-Policy "same-origin"
Header always set Cross-Origin-Resource-Policy "same-origin"
```

3L. Add Subresource Integrity to cross-origin scripts `Security`

- **Impact:** Supply-chain integrity
- **Problem:** Security basics reports '2 of 2 cross-origin scripts lack an integrity attribute' (jsdelivr iframemanager and cookieconsent).
- **Solution:** Pin versions and add SRI hashes:

```
<script
src="https://cdn.jsdelivr.net/gh/orestbida/cookieconsent@3.0.1/dist
/cookieconsent.umd.js"
        integrity="sha384-…" crossorigin="anonymous" defer>
</script>
```

  Or self-host these two libraries.

3M. WordPress hardening: readme.html, install.php, wp-login.php `Security`

- **Impact:** Attack surface, information disclosure
- **Problem:** Security basics flags `readme.html` as public, `/wp-admin/install.php` as reachable, and login served on the default `/wp-login.php` path.
- **Solution:**
  - Delete or block `readme.html`:

```
<Files "readme.html">
  Require all denied
</Files>
```

  - Block the installer: `Redirect 403 /wp-admin/install.php`.
  - Move or rate-limit the login path (e.g. a custom login slug plus Cloudflare rate limiting / WAF rules).

3N. Fix structured data and tap targets `SEO`

- **Impact:** SEO, mobile usability
- **Problem:** PSI's SEO audits fail on `structuredData` (JSON-LD type reported as 'Unknown') and `tapTargets`.
- **Solution:**

    - Emit a valid `FAQPage` schema with `Question` / `Answer` pairs matching the on-page accordion content.
    - Ensure interactive controls are ≥24×24 px (WCAG 2.5.8) with adequate spacing; enlarge the header search and footer links.

3O. Reduce server technology disclosure `Best Practices`

- **Impact:** Information disclosure
- **Problem:** The `server: cloudflare` header is disclosed and security basics marks technology disclosure as a warn.
- **Solution:** If the origin is Kinsta, strip the origin `server` header at the edge and rely on Cloudflare's own header. This is low-impact — do not trade it for breaking caching.

3P. Add Referrer-Policy, Permissions-Policy, COOP, CORP `Security`

- **Impact:** Privacy, origin isolation
- **Problem:** `referrer-policy`, `permissions-policy`, `cross-origin-opener-policy`, and `cross-origin-resource-policy` are all missing.
- **Solution:**

```
Referrer-Policy: strict-origin-when-cross-origin
Permissions-Policy: geolocation=(), microphone=(), camera=()
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
```

3Q. Harden WordPress surface `Security`

- **Impact:** Attack surface, info disclosure
- **Problem:** `readme.html` is public, `/wp-admin/install.php` is reachable, and login is on the default `/wp-login.php` path.
- **Solution:**
    - Delete or block `readme.html`.
    - Block `/wp-admin/install.php` in `.htaccess`.
    - Move or rate-limit `/wp-login.php` (e.g. WAF rule, custom login slug).

3R. Add structured data `SEO`

- **Impact:** Rich results eligibility
- **Problem:** PSI fails `structuredData`; the single JSON-LD block is typed 'Unknown'.
- **Solution:** Emit `Organization` / `LocalBusiness` JSON-LD with name, address, and contact details for the accommodation business.

3S. Extend srcset coverage to all raster images `Performance`

- **Impact:** Image bytes, mobile LCP
- **Problem:** Only 32 of 43 raster images (74%) use `srcset` or `<picture>` ; the checklist flags this as a warning.
- **Solution:**
  - Add `srcset` / `sizes` to the remaining 11 images, especially the two unsized `menu-image-*.jpg` files.
  - Keep the existing 16 distinct widths but drop unused sizes to reduce upload storage.

3T. Remove the deprecated API usage `Best Practices`

- **Impact:** Lighthouse Best Practices (81)
- **Problem:** PSI's `deprecations` audit fails with 1 warning found.
- **Solution:**
  - Open the Lighthouse deprecations audit in DevTools to identify the API, then replace it with the modern equivalent (commonly `document.write` , synchronous XHR, or legacy `unload` handlers).

3U. Add structured data and enlarge tap targets `SEO`

- **Impact:** SEO score (85), rich results eligibility
- **Problem:** PSI lists `structuredData` and `tapTargets` as failing SEO audits; the page has 1 JSON-LD block whose type is reported as Unknown.
- **Solution:**
  - Emit valid `LocalBusiness` / `LodgingBusiness` JSON-LD with name, address, phone, geo and price range.
  - Increase tap target size to at least 48×48 px with adequate spacing for the header and footer navigation.