Audit Report: Avaleht - Restate

Website: https://restate.ee/
Date: 13.11.2026
Audit Coverage: 100% — all sources returned data
Confidence: high

Pages Audited (1 of 1):

- https://restate.ee/

Summary of results

Overall Score: 83 / 100
Status: **Needs Improvement**

What is pulling the score down

Signal	Points	Evidence
Security basics	−10	FAILED: Strict-Transport-Security, Clickjacking protection, X-Content-Type-Options
HTML validation	−2	7 W3C errors
Performance 96	−1.6	weighted 40% of 4 points lost
Accessibility 95	−1.5	weighted 30% of 5 points lost
SEO 92	−1.2	weighted 15% of 8 points lost
Image delivery	−1	PSI estimates 495 KiB image-delivery savings (mobile)
Advanced security headers	0	Failing: Content-Security-Policy present, CSP is strict, Referrer-Policy, Permissions-Policy, Cross-Origin-Opener-Policy, Cross-Origin-Resource-Policy
Page score	**83**	100 − 17.3 → 83

Security basics FAILED (−10: HSTS, clickjacking protection and X-Content-Type-Options all missing) is by far the largest deduction; 7 W3C errors (−2) and 495 KiB of

estimated image-delivery savings (−1) follow, while mobile Performance 96 and field LCP 887 ms are already strong.

Per-page scores

 Needs Improvement · https://restate.ee/

Base	Score	Performance	Accessibility	Best Practices	SEO	Security
96	83	96	95	100	92	FAILED

PageSpeed Insights — Mobile vs Desktop

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

Strategy	Performance (M / D)	LCP (M / D)	CLS (M / D)
Mobile vs Desktop	**96** / 100	**2.57 s** / 610 ms	0.000 / 0.000

Optimization Checklist

6 of 7 passing — 6 pass · 0 warn · 1 fail · 1 n/a

Item	Status	Detail
Page caching plugin / CDN active	**Pass**	Caching plugin detected (WP Rocket)
Response compressed (gzip / brotli)	**Pass**	Document response is compressed with gzip.
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	N/A	No CSS background-images detected on raster-image-eligible elements.

Item	Status	Detail
background-image)		
Responsive images (srcset /)	**Pass**	6/6 raster images use srcset or (100%).
Reasonable number of image sizes	**Pass**	6 distinct srcset widths.
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. Add baseline security headers (HSTS, X-Frame-Options, X-Content-Type-Options) `Security`

- **Impact:** Security basics row (−10), Transport security, clickjacking, MIME sniffing
- **Problem:** The Security basics verdict is FAILED because Strict-Transport-Security, clickjacking protection and X-Content-Type-Options are all missing from the response.
- **Solution:** Send these from the origin (Apache example):

  ```
  Header always set Strict-Transport-Security "max-age=31536000;
  includeSubDomains"
  Header always set X-Content-Type-Options "nosniff"
  Header always set X-Frame-Options "SAMEORIGIN"
  ```

  If you later add a CSP, prefer `frame-ancestors 'self'` over X-Frame-Options.

1B. Fix W3C validation errors `Best Practices`

- **Impact:** HTML validation row (−2), HTML validity, parser robustness
- **Problem:** The W3C validator reports 7 errors, all of the same kind: a `<script>` with a non-JavaScript `type` (WP Rocket's `text/rocketlazyloadscript`) also carrying `defer`, first at line 957.
- **Solution:**

- Let WP Rocket rewrite the tag without `defer`, or exclude that script from delay/combination so the emitted markup is valid.
- Remove the redundant `type="text/javascript"` flagged as a warning at line 747.
- Re-run the validator after the plugin setting change to confirm 0 errors.

Priority 2: Important

Essential for compliance, user reach, and search visibility.

2A. Serve images in WebP/AVIF at the right size `Performance`

- **Impact:** Image delivery row (−1), Image bytes, LCP
- **Problem:** PSI estimates 495 KiB of image-delivery savings on mobile, and the runtime capture shows 590.6 KB of images across only 6 requests — the footer PNGs (hammer, lego, lollipop, chicken-dollar, croc, duck) are large raster files.
- **Solution:**
  - Re-encode the PNGs as WebP/AVIF and serve via `<picture>` with a PNG fallback.
  - Keep the existing `srcset` widths but cap the largest variant to the rendered size.

```
<picture>
  <source type="image/webp" srcset="hammer-233.webp 233w, hammer-
466.webp 466w" sizes="233px">
  <img src="hammer.png" alt="" width="233" height="382"
loading="lazy">
</picture>
```

2B. Load the hero image eagerly `Performance`

- **Impact:** LCP
- **Problem:** The optimization checklist fails on hero loading: the first/largest image (`hammer.png`) is served with `loading="lazy"` and no `fetchpriority`, which delays LCP (2.6 s lab on mobile).
- **Solution:**

```
<img src=".../hammer.png" alt="" width="233" height="382"
loading="eager" fetchpriority="high">
```

  Verify visually which element is the real LCP candidate before applying — the heuristic picks the first large `<img>`.

2C. Add a meta description `SEO`

- **Impact:** SEO, SERP snippet quality
- **Problem:** The document has no meta description (`meta-description` audit scores 0) and the HTML inventory confirms `Description: not set` .
- **Solution:** Add a unique 120–155 character description in the page head:

```
<meta name="description" content="Restate – kinnisvara arendus ja varahaldus Eestis. Tutvu meie kodude, äripindade ja aktiivsete pakkumistega.">
```

2D. Enlarge touch targets `Accessibility`

- **Impact:** Mobile usability, WCAG 2.5.8
- **Problem:** Lighthouse `target-size` scores 0.00 (weight 7) on mobile — interactive elements are smaller or closer than the 24×24 px minimum.
- **Solution:**
  - Give icon links and footer navigation items at least 44×44 px hit area via padding or `min-height` / `min-width` .
  - Add spacing between adjacent links so targets do not overlap.

Priority 3: Best Practice

Recommended for long-term maintainability.

3A. Give repeated landmarks unique accessible names `Accessibility`

- **Impact:** Screen-reader navigation
- **Problem:** axe-core reports one moderate `landmark-unique` violation on `.footer__social` : multiple landmarks share the same role without distinguishing labels.
- **Solution:**

```
<nav class="footer__social" aria-label="Sotsiaalmeedia">…</nav>
```

  Ensure every repeated `nav` / `aside` / `form` landmark has a distinct `aria-label` or `aria-labelledby` .

3B. Make link text descriptive `Accessibility`

- **Impact:** Link purpose (WCAG 2.4.4)
- **Problem:** The inventory lists repeated vague anchors — "ülevaade" ×4, "tiim" ×3, "äri" ×2, "kodud" ×2, "võta ühendust" ×2 — which are ambiguous out of context.
- **Solution:**

- Rewrite anchors to describe the destination (e.g. "Kodude ülevaade", "Tiimi tutvustus").
- Where visual design forbids longer text, add `aria-label` to disambiguate.

3C. Add structured data `SEO`

- **Impact:** Rich results eligibility
- **Problem:** The `structuredData` audit fails and the single JSON-LD block is typed "Unknown", so search engines get no usable entity markup.
- **Solution:** Emit valid schema.org JSON-LD, e.g. `Organization` plus `WebSite`:

```
<script type="application/ld+json">
{"@context":"https://schema.org","@type":"Organization","name":"Res
tate","url":"https://restate.ee/"}
</script>
```

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

- **Impact:** Information leakage, cross-origin isolation
- **Problem:** Referrer-Policy, Permissions-Policy, Cross-Origin-Opener-Policy and Cross-Origin-Resource-Policy are all missing; the advanced-headers row is currently scored as not warranted for this site type, so this is hardening rather than a must-fix.
- **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"
```

3E. Harden the Content-Security-Policy `Security`

- **Impact:** XSS defense-in-depth
- **Problem:** No Content-Security-Policy is sent. The site has no auth, payments or user-generated content, so XSS impact is limited and this stays a best practice rather than a must-fix.
- **Solution:** Deploy a nonce-based policy rather than a flat allowlist:

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

Note the two jsDelivr scripts and Google Fonts will need nonces or self-hosting.

3F. Add Subresource Integrity to third-party scripts `Security`

- **Impact:** Supply-chain tampering
- **Problem:** Both cross-origin scripts (jsDelivr iframemanager and cookieconsent) lack an `integrity` attribute.
- **Solution:**

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

  Pin exact versions and generate the hash from the fetched file.

3G. Hide server version headers `Security`

- **Impact:** Fingerprinting
- **Problem:** The response discloses `Server: Apache / ZoneOS`, and the Security basics technology-disclosure check is a warning.
- **Solution:**

```
ServerTokens Prod
ServerSignature Off
Header unset X-Powered-By
```

3H. Protect the WordPress login and installer `Security`

- **Impact:** Brute force, takeover path
- **Problem:** `/wp-admin/install.php` is reachable and the login form is served on the default `/wp-login.php` path.
- **Solution:**
  - Block the installer in `.htaccess`:

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

  - Add login rate limiting / 2FA and consider moving the login path behind a plugin or basic auth.