Audit Report: Avaleht - estply

Website: https://estply.com/
Date: 29.10.2026
Audit Coverage: 100% — all sources returned data
Confidence: high

Pages Audited (1 of 1):

- https://estply.com/

Summary of results

Overall Score: 80 / 100
Status: **Needs Improvement**

Performance is genuinely strong — PSI mobile 96 / desktop 98, LCP 2.4 s, CLS 0.008, TBT 0 ms, TTFB 3 ms — so the score is not dragged by speed. The real drags are image weight (8 image requests totalling 2.70 MB of a 2.76 MB page, with PSI estimating 276 KiB of delivery savings) and accessibility gaps that axe missed but Lighthouse caught: `button-name` (weight 10, score 0) and `target-size` (weight 7, score 0) pull mobile accessibility to 91. SEO is docked for a missing meta description, and W3C reports 12 errors (6–20 band) mostly from WP Rocket lazyload script types, an empty `href` on a dns-prefetch link, and malformed `srcset` / `sizes` pairs. Security basics PASS, but the advanced tier fails on CSP strictness (only `frame-ancestors 'self'`, no `default-src` / `object-src 'none'`), missing Referrer-Policy/Permissions-Policy/COOP/CORP, and HSTS without preload — none of which are P1 for a brochure site with no auth or payments. Confidence is high: every tool returned data and the signals are consistent.

Per-page scores

 Needs Improvement · https://estply.com/

Score	Performance	Accessibility	Best Practices	SEO	Security
80	96	91	81	92	PASS

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** / 98	**2.40 s** / 1.04 s	**0.008** / 0.001

Optimization Checklist

7 of 7 passing — 7 pass · 0 warn · 0 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	**Pass**	Hero image is eagerly loaded with fetchpriority="high" (inferred from DOM order/size — Lighthouse LCP element unavailable).
Hero is a real (not a CSS background-image)	N/A	No CSS background-images detected on raster-image-eligible elements.
Responsive images (srcset /)	**Pass**	7/7 raster images use srcset or (100%).
Reasonable number of image sizes	**Pass**	27 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. Give icon buttons an accessible name `Accessibility`

- **Impact:** WCAG 4.1.2 Name, Role, Value; Lighthouse accessibility score

- **Problem:** Lighthouse `button-name` scores 0.00 with weight 10 on mobile — buttons render without any accessible name, which is the single largest accessibility deduction (mobile 91 vs desktop 96).
- **Solution:** Add a text alternative to every button that has no visible label:

```
<button type="button" class="menu-toggle" aria-label="Open menu">
  <svg aria-hidden="true" focusable="false">…</svg>
</button>
```

  - Prefer visible text where design allows; otherwise `aria-label` or a visually-hidden `<span>`.
  - Mark decorative SVGs `aria-hidden="true"` so they don't become the name.

1B. Cut image payload (2.70 MB across 8 requests) `Performance`

- **Impact:** LCP, Speed Index, total page weight
- **Problem:** Browser runtime shows 2.70 MB of images out of 2.76 MB total, and PSI's `image-delivery-insight` estimates 276 KiB of savings; two 251×134 PNGs are still served as PNG.
- **Solution:**
  - Convert remaining PNG/JPEG assets to WebP/AVIF (the hero is already WebP — extend that to the rest).
  - Re-encode the two `…6c041c12….png` / `…f2870486….png` logos as SVG or WebP.
  - Trim the srcset ladder: 27 distinct widths is far more than needed; 4–5 breakpoints per image is enough.
  - Verify the largest hero variant is not being downloaded on mobile.

Priority 2: Important

Essential for compliance, user reach, and search visibility.

2A. Enlarge touch targets to 44×44 px `Accessibility`

- **Impact:** WCAG 2.5.8 Target Size; mobile usability
- **Problem:** Lighthouse `target-size` scores 0.00 (weight 7) — interactive elements do not meet minimum size or spacing on mobile.
- **Solution:**
  - Ensure every link/button hit area is at least 44×44 CSS px.
  - Add padding rather than growing the icon:

```
.icon-link { display:inline-flex; align-items:center; justify-content:center; min-width:44px; min-height:44px; }
```

- Check the footer link cluster and the header nav specifically.

2B. Add a meta description `SEO`

- **Impact:** Search snippet CTR, Lighthouse SEO (92)
- **Problem:** HTML inventory reports `Description: not set` and Lighthouse `meta-description` scores 0.00.
- **Solution:** Add a unique 120–155 character description per page:

```
<meta name="description" content="ESTPLY toodab kvaliteetset kasevineeri Jõgevamaal – kaasaegne vineeritehas Lemeks Grupi koosseisus.">
```

  In WordPress, set it via Yoast/Rank Math rather than hard-coding in the theme.

2C. Harden the Content-Security-Policy `Security`

- **Impact:** XSS defense-in-depth
- **Problem:** CSP is present but only `frame-ancestors 'self'` — no `default-src`, no `object-src 'none'`, so it restricts nothing about scripts or resources.
- **Solution:** Build a nonce-based policy rather than a flat allowlist:

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

  - Roll out in `Content-Security-Policy-Report-Only` first and fix violations before enforcing.
  - Note: the site has no login, checkout, or genuine user-content surface (the "upload" signal is a `wp-content/uploads` asset link), so this is defense-in-depth, not an active exposure.

2D. Fix the 12 W3C validation errors `Best Practices`

- **Impact:** Markup correctness, image loading behavior
- **Problem:** W3C reports 12 errors: 5× `defer` on `type="text/rocketlazyloadscript"` data blocks, an empty `href` on a dns-prefetch `<link>`, `src` on `<source>`, `sizes` starting with `auto` on a non-lazy image, and two `srcset` candidates missing width descriptors.
- **Solution:**
  - Remove the empty prefetch link or give it a real host:

```
<link rel="dns-prefetch" href="//cdn.jsdelivr.net">
```

- Drop `defer` / `async` from `type="text/rocketlazyloadscript"` blocks (they are data blocks, not scripts).
- Replace `src` with `srcset` on `<source>` elements.
- Add `loading="lazy"` to the image whose `sizes` starts with `auto`, or drop the `auto` prefix.
- Add width descriptors to every `srcset` candidate where `sizes` is present, e.g. `srcset="…-251x134.png 251w"`.

Priority 3: Best Practice

Recommended for long-term maintainability.

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

- **Impact:** Information leakage, feature abuse, origin isolation
- **Problem:** All four headers are missing; the security tool flags them as low-severity advanced-tier gaps.
- **Solution:**

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

3B. Add HSTS preload and SRI on the CDN script `Security`

- **Impact:** Transport hardening, third-party script integrity
- **Problem:** HSTS is `max-age=31536000; includeSubDomains` but lacks `preload`; the single cross-origin script (`cdn.jsdelivr.net/…/iframemanager.js`) has no `integrity` attribute.
- **Solution:**
  - Append `; preload` to the HSTS header, then submit the domain at hstspreload.org.
  - Pin the CDN script:

```
<script
src="https://cdn.jsdelivr.net/gh/orestbida/iframemanager@1.3.0/dist
/iframemanager.js"
        integrity="sha384-…" crossorigin="anonymous" defer>
</script>
```

- Better: self-host the 2.7 KB library and drop the third-party origin entirely.

3C. Reduce render-blocking CSS and unused rules `Performance`

- **Impact:** FCP, Speed Index (3.68 s mobile)
- **Problem:** PSI flags `render-blocking-insight` (est. 740 ms savings) and `unused-css-rules` (32 KiB); the 34.3 KB `global.css` is the only blocking stylesheet.
- **Solution:**
  - Inline the critical above-the-fold CSS and load the rest with `media="print" onload="this.media='all'"`.
  - Purge unused rules from `global.3578d4f092e5450b.css` (32 KiB unused).
  - WP Rocket can do "Remove Unused CSS" — enable it and verify the hero renders correctly.

3D. Block the WordPress installer and move the login path `Best Practices`

- **Impact:** Attack surface
- **Problem:** Security basics flags `/wp-admin/install.php` as reachable and the login form on the default `/wp-login.php` path.
- **Solution:**

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

  - Put `/wp-login.php` behind a WAF rule, IP allowlist, or a plugin that renames it.
  - Also strip the `Server: Apache / ZoneOS` header (`ServerTokens Prod`, `ServerSignature Off`).

3E. Verify contrast on the 9 undetermined nodes and disambiguate repeated link text `Accessibility`

- **Impact:** WCAG 1.4.3, 2.4.4
- **Problem:** axe returned 0 violations but could not determine contrast on 9 nodes (gradients/alpha), and 8 link labels repeat verbatim ("meist" ×2, "tooted" ×2, "kontakt" ×2, etc.).
- **Solution:**
  - Manually check the 9 flagged nodes against 4.5:1 (3:1 for large text) using DevTools' contrast picker.

- Disambiguate repeated nav/footer links with `aria-label` or visually-hidden context, e.g. `<a href="/meist/">meist<span class="sr-only"> – ettevõtte tutvustus</span></a>`.