Audit Report: Avaleht - estply

Website: https://estply.com/
Date: 28.10.2026
Audit Coverage: 100% — all sources returned data
Confidence: medium

Pages Audited (5 of 5):

- https://estply.com/
- https://estply.com/en/2026/07/06/vineeri-kvaliteediklassid-selgeks
- https://estply.com/kontakt
- https://estply.com/meist/tootmine-ja-tehnoloogia
- https://estply.com/liitu-meiega

Summary of results

Overall Score: 64 / 100
Status: **Needs Improvement**

Site overall 64 is the mean of 5 pages. Scores range 60 (https://estply.com/en/2026/07/06/vineeri-kvaliteediklassid-selgeks) → 68 (https://estply.com/kontakt). Weakest page: Mobile PSI performance is 62 against desktop 92 — a 30-point gap driven almost entirely by CLS 0.491 on mobile (desktop 0.144), with the footer element accounting for a 0.481 shift; LCP 3.9 s and Speed Index 4.81 s add further drag. Accessibility scores 91/96 but the structural picture is worse than the number suggests: the page has zero headings of any level (h1 ×0 through h6 ×0), axe flags page-has-heading-one, and Lighthouse fails button-name (score 0.00, weight 10) and target-size (score 0.00, weight 7). Security basics returned FAILED — HSTS, X-Frame-Options/frame-ancestors, X-Content-Type-Options, CSP, Referrer-Policy, Permissions-Policy, COOP and CORP are all missing, and 2 of 2 cross-origin scripts lack SRI — which caps the overall below 90. W3C reports 7 errors (5× `defer` on WP Rocket's `text/rocketlazyloadscript` data blocks, 2× srcset candidates missing width descriptors) and the document is served with `cache-control: max-age=0`, so repeat visits revalidate every time. Image assets are a minor factor here (only 2 raster PNGs, both lazy-loaded including the hero, no WebP), and SEO is otherwise clean at 100 with valid canonical, hreflang and 13 OG tags.

Per-page scores

 Needs Improvement · https://estply.com/

Score	Performance	Accessibility	Best Practices	SEO	Security
63	67	91	100	92	FAILED

 Needs Improvement · https://estply.com/en/2026/07/06/vineeri-kvaliteediklassid-selgeks

Score	Performance	Accessibility	Best Practices	SEO	Security
60	62	91	100	100	FAILED

 Needs Improvement · https://estply.com/kontakt

Score	Performance	Accessibility	Best Practices	SEO	Security
68	71	92	100	92	FAILED

 Needs Improvement · https://estply.com/meist/tootmine-ja-tehnoloogia

Score	Performance	Accessibility	Best Practices	SEO	Security
64	62	91	100	92	FAILED

 Needs Improvement · https://estply.com/liitu-meiega

Score	Performance	Accessibility	Best Practices	SEO	Security
65	64	92	100	92	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://estply.com/	**67** / 81	**6.15 s** / 2.50 s	**0.006** / 0.001
https://estply.com/en/2026/07/06/vineeri-kvaliteediklassid-selgeks	**62** / 92	**3.90 s** / 824 ms	**0.491** / 0.144

URL	Performance (M / D)	LCP (M / D)	CLS (M / D)
https://estply.com/kontakt	**71** / 90	**4.40 s** / 943 ms	**0.014** / 0.001
https://estply.com/meist/tootmine-ja-tehnoloogia	**62** / 89	**7.28 s** / 1.09 s	0.000 / **0.001**
https://estply.com/liitu-meiega	**64** / 90	**5.03 s** / 1.16 s	**0.099** / 0.001

Optimization Checklist

4 of 5 passing — 4 pass · 0 warn · 1 fail · 3 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 background-image)	N/A	No CSS background-images detected on raster-image-eligible elements.
Responsive images (srcset /)	N/A	Only 2 raster images on the page — responsive-image rule does not apply.
Reasonable number of image sizes	N/A	Too few raster images to evaluate srcset width variety.

Item	Status	Detail
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. Cut mobile LCP from 6.2 s `Performance`

- **Impact:** LCP, Speed Index, FCP, PSI mobile performance
- **Problem:** Mobile LCP is 6.2 s versus 2.5 s on desktop, and Speed Index is 7.03 s mobile versus 2.36 s desktop; PSI mobile performance is 67 against 81 desktop.
- **Solution:**
  - Preload the actual LCP image and keep `fetchpriority="high"` on it:

```
<link rel="preload" as="image" href="/wp-
content/uploads/2026/08/kaasik-kaupo-kalda-1-320x180.jpg"
imagesrcset="..." imagesizes="..." fetchpriority="high">
```

  - The hero is served at 320×180 with `sizes` / `srcset` — verify the browser is not picking a tiny candidate and upscaling, or a huge one and downscaling.
  - Add `font-display: swap` (PSI `font-display-insight` estimates 50 ms savings) and self-host the Open Sans woff2 currently pulled from fonts.gstatic.com.
  - Re-run PSI mobile after the image work; the 3.7 s mobile/desktop LCP delta points at payload + throttled CPU, not server response (TTFB 4 ms).

1B. Add the three missing baseline security headers `Security`

- **Impact:** Transport security, clickjacking, MIME sniffing
- **Problem:** Security basics verdict is FAILED: Strict-Transport-Security, X-Frame-Options/CSP frame-ancestors and X-Content-Type-Options are all missing. These are high-level hygiene checks on HTTP headers, TLS, cookies and a few well-known exposed paths. PASS means the basics are in place. It does **not** mean the site is secure: application logic, authentication, plugins, server configuration and dependencies are not tested here. Treat FAILED as a must-fix and PASS as a starting point, not a certificate.
- **Solution:** Send from the origin (Apache shown):

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

Then submit the domain at hstspreload.org once the max-age has been stable for a few weeks.

1C. Fix unnamed buttons and undersized touch targets `Accessibility`

- **Impact:** WCAG 4.1.2, 2.5.8; PSI accessibility 91 mobile
- **Problem:** PSI accessibility audits `button-name` (score 0.00, weight 10) and `target-size` (score 0.00, weight 7) both fail on mobile, dragging the category to 91.
- **Solution:**
  - Give every icon-only button an accessible name:

```
<button type="button" aria-label="Ava menüü"><svg aria-
hidden="true">…</svg></button>
```

  - Ensure interactive targets are at least 24×24 px (44×44 recommended) with adequate spacing — the cookie-consent and language-switcher controls are the usual offenders.
  - Re-check with keyboard-only navigation and a screen reader; axe reported 0 violations, so these are runtime/PSI-only failures.

1D. Eliminate the footer layout shift driving CLS 0.491 `Performance`

- **Impact:** CLS (mobile 0.491, desktop 0.144), Lighthouse performance score
- **Problem:** Lighthouse attributes a 0.481 shift to `div#page > div.main > div.main__footer > footer.footer` on mobile, pushing CLS to 0.491 — well past the 0.25 heavy-penalty threshold.
- **Solution:**
  - Reserve space for anything injected into the footer (cookie banner, iframe manager, late-loading badges) with explicit `min-height` or `aspect-ratio`.
  - If the footer shift comes from a web font swap, add `font-display: optional` or preload the Open Sans woff2 and self-host it instead of loading from `fonts.googleapis.com`.
  - Audit the footer for JS-injected nodes (WP Rocket lazyload, cookieconsent) that insert content above existing content — insert below or use `position: fixed` overlays.

- Re-run Lighthouse mobile after each change; target CLS ≤ 0.1.

1E. Add HSTS, clickjacking protection and nosniff `Security`

- **Impact:** Transport security, clickjacking, MIME sniffing
- **Problem:** Security basics verdict is FAILED: Strict-Transport-Security, X-Frame-Options/frame-ancestors and X-Content-Type-Options are all missing from the response headers.
- **Solution:** Send from the origin (Apache shown in the `Server` header):

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

  Prefer `Content-Security-Policy: frame-ancestors 'self'` over X-Frame-Options once CSP is in place, and verify HSTS preload status at hstspreload.org.

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

- **Impact:** LCP (3.9 s mobile), Speed Index (4.81 s)
- **Problem:** The optimized-web checklist fails 'Hero image eagerly loaded' — the first raster image (`uploads/2026/08/6c041c12…png`) carries `loading="lazy"` and no `fetchpriority`, delaying the mobile LCP to 3.9 s.
- **Solution:**

```
<img src="/wp-content/uploads/2026/08/6c041c12….png"
     alt="…" width="251" height="134"
     loading="eager" fetchpriority="high" decoding="async">
```

  Also add `<link rel="preload" as="image" href="…" fetchpriority="high">` in `<head>` and confirm the real LCP element in DevTools Performance panel.

1G. Restore document heading structure and name the buttons `Accessibility`

- **Impact:** WCAG 1.3.1 / 2.4.6, Lighthouse accessibility score
- **Problem:** The heading outline shows h1–h6 all at 0, axe flags page-has-heading-one, and Lighthouse fails `button-name` (score 0.00, weight 10).
- **Solution:**
  - Add exactly one `<h1>` containing the article title ("Vineeri kvaliteediklassid selgeks") and demote any visual-only titles to `<h2>` / `<h3>`.
  - Give every `<button>` an accessible name — visible text, `aria-label`, or `aria-labelledby`:

```
<button type="button" aria-label="Close cookie banner">…</button>
```

- Re-run axe to confirm 0 violations.

1H. Cut mobile document latency and Speed Index `Performance`

- **Impact:** Speed Index, FCP, LCP, TTFB
- **Problem:** Mobile Speed Index is 10.25 s (3.94 s desktop), the document request took 2.67 s in the runtime capture, and PSI's document-latency-insight estimates 4,360 ms of savings.
- **Solution:**
  - Confirm WP Rocket page cache is actually serving this URL (the response shows `cache-control: max-age=0`, i.e. no browser caching) and warm the cache after deploys.
  - Serve the document from a CDN edge close to Estonian/EU visitors.
  - Inline critical CSS and defer the 5 external stylesheets.
  - Self-host or preload the Open Sans woff2 (47.2 KB from fonts.gstatic.com) and add `font-display: swap` (font-display-insight, ~50 ms).
  - Remove the 18 KB of unused JS and the 12 `text/rocketlazyloadscript` blocks that never execute as scripts.

1I. Add baseline security headers (HSTS, X-Frame-Options, X-Content-Type-Options) `Security`

- **Impact:** Transport security, clickjacking, MIME sniffing
- **Problem:** Security basics verdict is FAILED: Strict-Transport-Security, X-Frame-Options/frame-ancestors and X-Content-Type-Options are all missing on the HTTPS response.
- **Solution:** Send from the origin (Apache shown in the `server` header):

  ```
  Header always set Strict-Transport-Security "max-age=63072000;
  includeSubDomains; preload"
  Header always set X-Content-Type-Options "nosniff"
  Header always set X-Frame-Options "SAMEORIGIN"
  Header always set Referrer-Policy "strict-origin-when-cross-origin"
  ```

  Then submit the domain to hstspreload.org once the max-age is stable.

1J. Deploy a nonce-based Content-Security-Policy `Security`

- **Impact:** XSS defense on a form that accepts user input
- **Problem:** No Content-Security-Policy header is present, and the contact page contains a textarea-based form, so user-supplied content reaches the application.

- **Solution:** Use nonce + `'strict-dynamic'` 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'; form-action 'self'
```

  - Generate a fresh nonce per response and stamp it on every `<script>`.
  - Roll out in `Content-Security-Policy-Report-Only` first to catch violations from the jsdelivr cookie-consent/iframe-manager bundles.

1K. Eager-load the hero image with high fetchpriority `Performance`

- **Impact:** LCP, Speed Index
- **Problem:** The hero image (…/2026/09/kaupokalda-com-dji_20260717125043_0188_d-528x396.jpg) carries loading="lazy" and no fetchpriority, and mobile LCP is 7.3 s versus 1.1 s on desktop.
- **Solution:**
  - Remove `loading="lazy"` from the hero and add `fetchpriority="high"`:

```
<img src="/wp-content/uploads/2026/09/hero-528x396.jpg"
     srcset="…" sizes="…"
     width="528" height="396"
     fetchpriority="high"
     alt="…">
```

  - Keep `loading="lazy"` only on below-the-fold images.
  - Preload the hero if it is discovered late:

```
<link rel="preload" as="image" href="/wp-
content/uploads/2026/09/hero-528x396.jpg" fetchpriority="high">
```

1L. Cut document latency and the redirect hop `Performance`

- **Impact:** TTFB, FCP, LCP, Speed Index
- **Problem:** The document-latency insight estimates 3,810 ms of savings, and the browser capture shows two document requests (3.83 s for the non-trailing-slash URL, 2.38 s for the trailing-slash URL) — a redirect plus slow origin response.
- **Solution:**
  - Serve the canonical trailing-slash URL directly; add a rewrite so `/meist/tootmine-ja-tehnoloogia` never 301s.
  - Enable full-page caching for this URL in WP Rocket and warm the cache after deploy.

    - Check origin PHP/DB time; the 3.8 s document fetch is server-side, not network.
    - Consider a CDN in front of the origin for HTML.

1M. Add baseline security headers (HSTS, X-Content-Type-Options, frame protection) `Security`

- **Impact:** Transport security, clickjacking, MIME sniffing
- **Problem:** Security basics FAILED: Strict-Transport-Security, X-Content-Type-Options and both X-Frame-Options / CSP frame-ancestors are missing.
- **Solution:** Send from the origin (Apache shown, matching the `Server: Apache / ZoneOS` header):

  ```
  Header always set Strict-Transport-Security "max-age=63072000;
  includeSubDomains; preload"
  Header always set X-Content-Type-Options "nosniff"
  Header always set X-Frame-Options "SAMEORIGIN"
  Header always set Referrer-Policy "strict-origin-when-cross-origin"
  ```

  Then submit the domain to hstspreload.org once HSTS is confirmed stable.

1N. Shorten the critical request chain (document latency) `Performance`

- **Impact:** LCP, FCP, Speed Index, TTFB-perceived
- **Problem:** Lighthouse's document-latency-insight estimates 3,860 ms of savings on mobile, and Speed Index is 9.39 s with 6 external stylesheets plus 3 inline blocks (9.6 KB) in the head.
- **Solution:**
    - Inline above-the-fold critical CSS and load the remaining 6 stylesheets with `media="print" onload="this.media='all'"` or `rel="preload" as="style"`.
    - Remove unused CSS/JS from the critical path (WP Rocket's "Remove Unused CSS" / delay-JS options).
    - Preconnect is already present for fonts; verify it fires before the stylesheet request.

1O. Add HSTS, X-Content-Type-Options and clickjacking protection `Security`

- **Impact:** Transport security, MIME sniffing, clickjacking
- **Problem:** Security basics verdict is FAILED: Strict-Transport-Security, X-Content-Type-Options and both X-Frame-Options / CSP frame-ancestors are missing, so the page can be framed.
- **Solution:**

```
Header always set Strict-Transport-Security "max-age=31536000;
includeSubDomains; preload"
Header always set X-Content-Type-Options "nosniff"
Header always set X-Frame-Options "SAMEORIGIN"
Header always set Referrer-Policy "strict-origin-when-cross-origin"
Header always set Permissions-Policy "geolocation=(), microphone=
(), camera=()"
```

Then submit the domain to hstspreload.org once the max-age is stable.

Priority 2: Important

Essential for compliance, user reach, and search visibility.

2A. Shrink the 2.30 MB image payload `Performance`

- **Impact:** Page weight, LCP, Speed Index
- **Problem:** 8 images account for 2.30 MB of the 2.43 MB total page weight, and PSI's `image-delivery-insight` estimates 513 KiB of savings.
- **Solution:**
  - Serve WebP/AVIF with a raster fallback via `<picture>`; the two 251×134 PNGs (`6c041c12…png`, `f2870486…png`) are prime candidates.
  - Right-size the hero: a 320×180 JPEG is being used as the LCP element, so either supply a properly sized large candidate or stop upscaling it.
  - Keep the existing `srcset` / `loading="lazy"` setup — the optimized-web checklist already passes 7/7 on responsive images and lazy loading.

2B. Add a meta description `SEO`

- **Impact:** SEO 92, SERP snippet quality
- **Problem:** The document has no meta description (`meta-description` audit score 0.00) and PSI SEO sits at 92 on both strategies.
- **Solution:** Add a unique, ~150-character description per language variant:

```
<meta name="description" content="ESTPLY toodab kvaliteetset
kasevineeri Jõgevamaal – kaasaegne vineeritehas ja usaldusväärne
partner Sinu ärile.">
```

Repeat for the `/en/` hreflang variant.

2C. Add a nonce-based Content-Security-Policy `Security`

- **Impact:** XSS defense-in-depth
- **Problem:** CSP is missing entirely. Site signals flag user-generated content (an anchor href contains "upload"), but the page itself is a brochure with no forms, no

auth and no checkout, so this is calibrated to P2 rather than P1.

- **Solution:** Deploy a nonce + `strict-dynamic` policy rather than a flat allowlist:

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

Note the site loads scripts from cdn.jsdelivr.net (iframemanager, cookieconsent) — `'strict-dynamic'` covers those once the loader is nonced. Roll out in report-only mode first.

2D. Harden WordPress entry points `Security`

- **Impact:** Takeover path, brute-force surface
- **Problem:** `/wp-admin/install.php` is reachable and the login form is served on the default `/wp-login.php` path.
- **Solution:**

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

  - Move or protect the login path (WPS Hide Login or an IP allowlist on `/wp-login.php`).
  - Add rate limiting / 2FA on the login endpoint.
  - The remaining WordPress checks (xmlrpc blocked, no version disclosure, no user enumeration, no directory listing, no debug.log) already pass.

2E. Add Subresource Integrity to cross-origin scripts `Best Practices`

- **Impact:** Supply-chain integrity
- **Problem:** 2 of 2 cross-origin scripts — `iframemanager@1.3.0` and `cookieconsent@3.0.1` from cdn.jsdelivr.net — lack `integrity` attributes.
- **Solution:**

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

Generate the hash with `openssl dgst -sha384 -binary file.js | openssl base64 -A`, or self-host both libraries.

2F. Verify contrast on the 17 undetermined nodes `Accessibility`

- **Impact:** WCAG 1.4.3
- **Problem:** axe returned 0 violations but flagged 17 nodes where it could not compute contrast (alpha transparency or gradients), so the real contrast state is unverified.
- **Solution:**
  - Inspect the 17 nodes in DevTools with the contrast checker, sampling the actual rendered background.
  - Target ≥4.5:1 for body text and ≥3:1 for large text.
  - Also confirm visible focus indicators and modal focus trapping manually — axe cannot verify either.

2G. Stop serving the document with cache-control: max-age=0 `Performance`

- **Impact:** TTFB on repeat visits, FCP, LCP
- **Problem:** The HTML response returns `cache-control: max-age=0` with `expires` set to the same second, so every navigation revalidates despite WP Rocket being active.
- **Solution:**
  - Configure WP Rocket / the server to send a short but non-zero TTL for HTML, e.g. `Cache-Control: public, max-age=600, s-maxage=3600`.
  - Keep `Vary: Accept-Encoding` and add `ETag` so conditional requests work.
  - Ensure logged-in / admin paths bypass the cache.

2H. Enlarge touch targets `Accessibility`

- **Impact:** WCAG 2.5.8, Lighthouse target-size audit
- **Problem:** Lighthouse fails `target-size` (score 0.00, weight 7) on mobile and the modeled SEO audit `tapTargets` also fails.
- **Solution:**
  - Ensure every interactive element is at least 44×44 px with ≥8 px spacing.
  - Add padding to icon links and footer navigation items rather than relying on the glyph size:

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

2I. Fix the 7 W3C validation errors `Best Practices`

- **Impact:** HTML validity, script execution order, responsive image selection

- **Problem:** W3C reports 7 errors: 5× `defer` on `<script type="text/rocketlazyloadscript">` data blocks (first at line 23) and 2× srcset candidates with no width descriptor (lines 563, 583).
- **Solution:**
  - WP Rocket's lazyload rewrites `type` to a non-JS MIME type; exclude the cookieyes/iframemanager snippets from 'Delay JS execution' or move `defer` handling into the plugin's own loader.
  - Add width descriptors to every srcset candidate when `sizes` is present:

```
<img src="…251x134.png"
     srcset="…251x134.png 251w, …502x268.png 502w"
     sizes="(max-width: 600px) 100vw, 251px"
     width="251" height="134" alt="">
```

2J. Add Referrer-Policy and Permissions-Policy `Security`

- **Impact:** Referrer leakage, feature exposure
- **Problem:** Both Referrer-Policy and Permissions-Policy are missing from the response headers (flagged low in the header scan, but cheap to add).
- **Solution:**

```
Header always set Referrer-Policy "strict-origin-when-cross-origin"
Header always set Permissions-Policy "geolocation=(), microphone=
(), camera=(), interest-cohort=()"
```

2K. Give buttons accessible names and enlarge touch targets `Accessibility`

- **Impact:** WCAG 4.1.2 Name/Role/Value, 2.5.8 Target Size
- **Problem:** PSI accessibility fails `button-name` (score 0.00, weight 10) and `target-size` (score 0.00, weight 7) on mobile, even though axe-core reported 0 violations.
- **Solution:**
  - Add visible text or `aria-label` to every icon-only button, e.g. `<button aria-label="Ava menüü">`.
  - Ensure interactive targets are at least 24×24 CSS px (44×44 recommended) with adequate spacing:

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

  - Verify keyboard focus is visible on all controls.

2L. Add a meta description and valid structured data `SEO`

- **Impact:** Search snippet quality, rich results
- **Problem:** The document has no meta description and PSI's `structuredData` audit fails; the single JSON-LD block is typed "Unknown".
- **Solution:**
  - Add a unique Estonian description (~150 chars) and a matching English one on /en/contact/:

```
<meta name="description" content="Võta ühendust Estply meeskonnaga
— logistika, laadimine ja kontaktandmed.">
```

  - Replace the untyped JSON-LD with a valid `Organization` + `ContactPage` graph including `name`, `url`, `email`, `telephone` and `address`.

2M. Fix the 17 W3C validation errors `Best Practices`

- **Impact:** Markup correctness, lazy-load reliability, image selection
- **Problem:** W3C reports 17 errors: 12× `script type="text/rocketlazyloadscript"` carrying `defer`, 2× hidden inputs with `autocomplete`, 1× `charset` after the first 1024 bytes, and 2× `srcset` candidates missing width descriptors.
- **Solution:**
  - Drop `defer` from the Rocket Loader data-block scripts (they are not executable scripts):

```
<script type="text/rocketlazyloadscript" data-rocket-
type="text/javascript" id="cookieyes">
```

  - Remove `autocomplete` from `<input type="hidden">` elements.
  - Move `<meta charset="utf-8">` into the first 1024 bytes of `<head>`.
  - Add width descriptors to the two offending `srcset` values:

```
<img srcset="/img/a-400.png 400w, /img/a-800.png 800w" sizes="(max-
width: 768px) 100vw, 50vw" …>
```

2N. Enable browser caching for the document and static assets `Performance`

- **Impact:** Repeat-visit TTFB, Speed Index
- **Problem:** The document response sends `cache-control: max-age=0` with an `expires` value equal to the request time, so nothing is reused between visits despite WP Rocket being active.

- **Solution:**
  - Let WP Rocket serve cached HTML with a short TTL plus `stale-while-revalidate`:

```
Cache-Control: public, max-age=600, stale-while-revalidate=86400
```

  - Set long-lived immutable caching for hashed assets:

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

  - Keep `max-age=0` only for logged-in or form-submission responses.

2O. Fix document caching and self-host fonts `Performance`

- **Impact:** Repeat-visit TTFB, FCP, render delay
- **Problem:** The document is served with `cache-control: max-age=0` and `expires` in the past, and Google Fonts add two third-party origins (47.2 KB from fonts.gstatic.com) with a `font-display` insight estimating 110 ms of savings.
- **Solution:**
  - Allow short-lived HTML caching at the edge, e.g. `Cache-Control: public, max-age=600, s-maxage=3600, stale-while-revalidate=86400`.
  - Self-host Open Sans as woff2 with `font-display: swap` and `<link rel="preload" as="font" type="font/woff2" crossorigin>`, removing fonts.googleapis.com / fonts.gstatic.com from the critical path.

2P. Harden the WordPress install surface `Security`

- **Impact:** Brute-force and takeover risk
- **Problem:** Security basics reports `/wp-admin/install.php` reachable and the login form on the default `/wp-login.php` path; 2 of 2 cross-origin scripts (jsDelivr) lack Subresource Integrity.
- **Solution:**
  - Block the installer in `.htaccess`:

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

  - Move or protect the login path (custom login slug, or IP/2FA restriction) and rate-limit `/wp-login.php`.
  - Add `integrity` + `crossorigin` to the jsDelivr `<script>` tags, or self-host those libraries.

2Q. Fix font loading (font-display + preload) `Performance`

- **Impact:** FCP, LCP, CLS
- **Problem:** font-display-insight estimates 120 ms of savings, and 47.2 KB of Open Sans is fetched from fonts.gstatic.com as the single largest third-party resource.
- **Solution:**
  - Add `&display=swap` to the Google Fonts URL.
  - Preload the primary woff2 and preconnect to fonts.gstatic.com (already present — verify it precedes the CSS request).
  - Consider self-hosting the 3 font files to remove the third-party round trip.

2R. Serve modern image formats (WebP/AVIF) `Performance`

- **Impact:** Page weight, LCP, Speed Index
- **Problem:** All 31 raster images are JPEG (260.9 KB of the 372.7 KB runtime page weight) with no WebP or AVIF variants, and 35 distinct srcset widths are generated.
- **Solution:**
  - Enable WebP/AVIF conversion in WP Rocket (or a plugin such as Imagify/ShortPixel) and keep the existing srcset.
  - Prune the 35 generated widths down to 4–5 meaningful breakpoints to cut origin storage and CDN churn.

2S. Reserve space for the hero block to eliminate layout shift `Performance`

- **Impact:** CLS
- **Problem:** Mobile CLS is 0.099, driven by a 0.099 shift on `div.hero-images__media > div.grid__col > div.hero-images__content > p`.
- **Solution:**
  - Give the hero media container an explicit `aspect-ratio` or min-height so the paragraph cannot reflow the layout.
  - Set `width` / `height` on the hero `<img>` (already present on other images) and avoid injecting content above it after load.

2T. Fix unnamed buttons and undersized touch targets `Accessibility`

- **Impact:** PSI accessibility (92 mobile), WCAG 2.5.8 / 4.1.2
- **Problem:** Lighthouse fails `button-name` (score 0.00) and `target-size` (score 0.00) on mobile, dragging accessibility to 92 despite axe reporting 0 violations.
- **Solution:**

- Add visible text or `aria-label` to every `<button>`, e.g. `<button aria-label="Ava menüü">`.
- Ensure interactive elements are at least 24×24 CSS px (44×44 recommended) with adequate spacing:

```
.icon-btn { min-width: 44px; min-height: 44px; }
```

2U. Fix the 18 W3C validation errors `Best Practices`

- **Impact:** HTML validity, script execution reliability
- **Problem:** W3C reports 18 errors: 13× `script type="text/rocketlazyloadscript"` combined with `defer`, 2× hidden input with `autocomplete`, 1× charset declared after the first 1024 bytes, and 2× srcset candidates missing a width descriptor.
- **Solution:**
  - Move `<meta charset="utf-8">` to the very first bytes of `<head>` (currently at line 6, after a script).
  - Remove `defer` from the 13 WP Rocket `text/rocketlazyloadscript` tags, or switch to `type="text/javascript"` with `defer`.
  - Drop `autocomplete` from hidden inputs.
  - Add width descriptors to the two srcset values flagged at lines 2637 and 2657:

```
<img srcset="...-300x200.png 300w, ...-1024x683.png 1024w" sizes="
(max-width: 1024px) 100vw, 1024px">
```

2V. Stop serving the HTML document with cache-control: max-age=0 `Performance`

- **Impact:** TTFB, repeat-visit LCP
- **Problem:** The document response returns `cache-control: max-age=0` even though WP Rocket 3.23.5.1 is detected, so every visit revalidates the 225 KB HTML.
- **Solution:**
  - Configure WP Rocket page caching for this URL and confirm the response sends a positive `max-age` (or `s-maxage` at the CDN) with `Vary: Accept-Encoding`.
  - Verify the cache is warmed for the canonical URL after each deploy.

Priority 3: Best Practice

Recommended for long-term maintainability.

3A. Fix document caching `Performance`

- **Impact:** Repeat-visit TTFB, back/forward cache
- **Problem:** The HTML response sends `cache-control: max-age=0` with an `expires` equal to the request time, so the document is revalidated on every visit despite WP Rocket being active.
- **Solution:**
  - Let WP Rocket manage HTML caching and emit a short positive `max-age` (e.g. `max-age=600, public`) instead of `max-age=0`.
  - Keep `vary: Accept-Encoding` as-is; the gzip compression (ratio 0.244) is already working.

3B. Fix the 9 W3C validation errors `Best Practices`

- **Impact:** HTML validity, image srcset correctness
- **Problem:** W3C reports 9 errors: 5× `defer` on a `type="text/rocketlazyloadscript"` data block, an empty `href` on a dns-prefetch link, `sizes` starting with `auto` on a non-lazy image, and 2 srcset candidates missing width descriptors.
- **Solution:**
  - Remove `defer` from the RocketLazyload data blocks (they are not executable scripts).
  - Drop the empty `<link data-rocket-prefetch href="" rel="dns-prefetch">` or give it a real host.
  - Add `loading="lazy"` to the image whose `sizes` starts with `auto`, or remove the `auto` token.
  - Add width descriptors to the two PNG srcset candidates:

```
<img srcset="/…/6c041c12….png 251w" sizes="251px" …>
```

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

- **Impact:** SEO 92, rich results eligibility
- **Problem:** PSI flags `structuredData` and `tapTargets` as failing SEO audits; the single JSON-LD block is present but its type resolves to "Unknown".
- **Solution:**
  - Replace the untyped JSON-LD with a valid `Organization` + `WebSite` graph (name, url, logo, sameAs).
  - Increase spacing/size of small inline links so tap targets meet the 24 px minimum.

    - The hreflang set (en/et/x-default), canonical and robots directives are already correct.

3D. Add remaining hardening headers and suppress the Server banner `Security`

- **Impact:** Privacy, feature exposure, fingerprinting
- **Problem:** Referrer-Policy, Permissions-Policy, Cross-Origin-Opener-Policy, Cross-Origin-Resource-Policy and X-Permitted-Cross-Domain-Policies are all missing, and the response discloses `Server: Apache / ZoneOS`.
- **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"
Header always set X-Permitted-Cross-Domain-Policies "none"
ServerSignature Off
ServerTokens Prod
```

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

- **Impact:** XSS defense-in-depth
- **Problem:** Content-Security-Policy is missing entirely. Site signals show no auth, payments, user content or e-commerce on this page, so XSS impact is limited — hence P3 rather than P1.
- **Solution:** Deploy a nonce/hash CSP with `'strict-dynamic'` 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'
```

  Note the WordPress admin (`/wp-login.php`) is reachable, so revisit this as P1 if the site ever adds authenticated areas.

3F. Harden the WordPress install surface `Security`

- **Impact:** Attack surface, information disclosure
- **Problem:** Security basics warns that `/wp-admin/install.php` is reachable and the login form is on the default `/wp-login.php` path; the `Server` header also discloses `Apache / ZoneOS`.
- **Solution:**
    - Block the installer in `.htaccess`:

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

- Move or protect the login path (custom login slug plugin, or IP allowlist on `/wp-login.php`).
- Strip the version banner: `ServerTokens Prod` and `ServerSignature Off`.

3G. Add structured data and disambiguate repeated link text `SEO`

- **Impact:** Rich results eligibility, WCAG 2.4.4
- **Problem:** The modeled `structuredData` audit fails and the single JSON-LD block is typed 'Unknown'; the inventory also finds repeated vague anchors ("code of conduct" ×3, "about us" ×2, "products" ×2).
- **Solution:**
  - Emit a valid `Article` / `BlogPosting` JSON-LD block with `headline`, `datePublished`, `author` and `image`.
  - Disambiguate repeated links with `aria-label` or surrounding context, e.g. `<a href="/en/about/" aria-label="About estply">about us</a>`.

3H. Serve the two PNGs as WebP `Performance`

- **Impact:** Image bytes (29.3 KB), LCP candidate
- **Problem:** Both raster images on the page are PNG with no WebP/AVIF variant; total image bytes are 29.3 KB across 3 requests.
- **Solution:** Convert to WebP with a fallback:

```
<picture>
  <source type="image/webp" srcset="…webp">
  <img src="…png" width="251" height="134" alt="" loading="lazy">
</picture>
```

Low impact given only 2 images — do this alongside the hero/LCP work.

3I. Verify color contrast on the 109 undetermined nodes `Accessibility`

- **Impact:** WCAG 1.4.3 Contrast (Minimum)
- **Problem:** axe-core could not evaluate contrast on 109 nodes (gradients/alpha backgrounds), so the 0-violation result does not prove compliance.
- **Solution:**
  - Run a contrast check in DevTools on text over gradients and images.
  - Target ≥4.5:1 for body text and ≥3:1 for large text.

- Where text sits on photography, add a solid overlay or scrim rather than relying on the image.

3J. Harden remaining headers and WordPress surface `Security`

- **Impact:** Information disclosure, feature abuse, brute force
- **Problem:** Referrer-Policy, Permissions-Policy, COOP, CORP and X-Permitted-Cross-Domain-Policies are all missing; the `server` header discloses `Apache / ZoneOS`; `/wp-admin/install.php` is reachable and login sits on the default `/wp-login.php`.
- **Solution:**

```
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"
Header always set X-Permitted-Cross-Domain-Policies "none"
ServerSignature Off
ServerTokens Prod
```

  - Block the installer: `<Files "install.php">Require all denied</Files>`.
  - Move login behind a custom path or add rate limiting / 2FA.

3K. Disambiguate repeated vague link text `SEO`

- **Impact:** Anchor-text relevance, screen-reader navigation
- **Problem:** Repeated anchors such as "kontakt" ×3, "meist" ×2 and "tooted" ×2 give no context out of flow.
- **Solution:**
  - Make link text self-describing ("Võta meiega ühendust", "Loe meie kohta").
  - Where the visual design requires short labels, add `aria-label` with the full context.

3L. Fix W3C validation errors `Best Practices`

- **Impact:** Markup correctness, validator score
- **Problem:** W3C reports 7 errors: 5× `script type="text/rocketlazyloadscript"` combined with `defer`, and 2× `srcset` candidates missing width descriptors (lines 935, 955).
- **Solution:**
  - WP Rocket's lazyload placeholder script should not carry `defer`; exclude those snippets from delay or use the plugin's native delay method.
  - Add width descriptors to the two PNG `srcset` values:

```
<img srcset="/…/image-251x134.png 251w, /…/image-502x268.png 502w"
sizes="251px" …>
```

3M. Disambiguate repeated link text `Accessibility`

- **Impact:** Screen-reader link lists, WCAG 2.4.4
- **Problem:** The page repeats vague anchor text — "käitumiskoodeks" ×3, "meist" ×3, "tooted" ×2, "kontakt" ×2 — with no visible disambiguation.
- **Solution:**
  - Add `aria-label` with context, e.g. `<a href="/meist/tootmine-ja-tehnoloogia" aria-label="Meist – tootmine ja tehnoloogia">meist</a>`.
  - Or extend the visible text so each link is unique out of context.

3N. Manually verify the 27 undetermined color-contrast nodes `Accessibility`

- **Impact:** WCAG 1.4.3 contrast
- **Problem:** axe returned 0 violations but flagged 27 nodes as "incomplete" for color contrast, so contrast compliance is unconfirmed.
- **Solution:**
  - Run axe DevTools or Chrome DevTools contrast picker on those 27 nodes (likely text over images/gradients).
  - Target ≥4.5:1 for body text and ≥3:1 for large text; add a solid overlay behind text on imagery.

3O. Make structured data explicit `SEO`

- **Impact:** Rich results eligibility
- **Problem:** The single JSON-LD block parses as valid but its type is reported as "Unknown", and Lighthouse's `structuredData` audit fails.
- **Solution:**
  - Declare an explicit `@type` (e.g. `Organization`, `WebPage`, `JobPosting` for the careers content) and validate with the Rich Results Test.
  - Add `BreadcrumbList` for the /liitu-meiega/ path.