Audit Report: Avaleht - estply

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

Pages Audited (5 of 5):

- https://estply.com/
- https://estply.com/en/2026/07/06/vineeri-kvaliteediklassid-selgeks
- https://estply.com/en/privacy-policy
- https://estply.com/privaatsuspoliitika
- https://estply.com/kupsiste-poliitika

Summary of results

Overall Score: 74 / 100
Status: **Needs Improvement**

Site overall 74 is the mean of 5 pages. Scores range 68 (https://estply.com/en/2026/07/06/vineeri-kvaliteediklassid-selgeks) → 79 (https://estply.com/en/privacy-policy). Weakest page: PSI mobile 66 vs desktop 94 — a 28-point gap driven almost entirely by CLS 0.491 (footer shift 0.481) and LCP 3.8 s on mobile, both well outside the good band, while desktop CLS 0.138 and LCP 0.8 s are near-passing. TBT 0 ms and FCP 1.67 s show the main thread is healthy; the drag is layout instability plus a hero image served with loading="lazy" (optimized-web checklist fail) and a 1.56 s document request with ~1,980 ms estimated latency savings. Accessibility is close to clean — axe reports 1 moderate violation (page-has-heading-one) against 35 passes — but PSI flags button-name and target-size, and the HTML inventory shows zero h1–h6 elements, a genuine outline gap. Security basics PASS (HSTS, nosniff, framing, TLS, no mixed content), though the CSP is only frame-ancestors 'self' with no default-src or object-src 'none', and Referrer-Policy, Permissions-Policy, COOP and CORP are absent. W3C reports 8 errors, mostly WP Rocket's text/rocketlazyloadscript carrying defer/async plus two srcset entries missing width descriptors. Field CrUX values (0 ms p75 for LCP/TTFB/INP) look like missing/fallback data and were not used for scoring.

Per-page scores

 Needs Improvement · https://estply.com/

Score	Performance	Accessibility	Best Practices	SEO	Security
73	77	91	81	92	PASS

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

Score	Performance	Accessibility	Best Practices	SEO	Security
68	66	91	100	100	PASS

 Needs Improvement · https://estply.com/en/privacy-policy

Score	Performance	Accessibility	Best Practices	SEO	Security
79	87	91	100	85	PASS

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

Score	Performance	Accessibility	Best Practices	SEO	Security
74	87	91	100	92	PASS

 Needs Improvement · https://estply.com/kupsiste-poliitika

Score	Performance	Accessibility	Best Practices	SEO	Security
78	83	91	100	92	PASS

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/	**77** / 83	**4.80 s** / 2.72 s	0.000 / 0.000
https://estply.com/en/2026/07/06/vineeri-kvaliteediklassid-selgeks	**66** / 94	**3.79 s** / 803 ms	**0.491** / 0.138

URL	Performance (M / D)	LCP (M / D)	CLS (M / D)
https://estply.com/en/privacy-policy	**87** / 100	**3.86 s** / 819 ms	0.000 / 0.000
https://estply.com/privaatsuspoliitika	**87** / 99	**3.90 s** / 833 ms	0.000 / 0.000
https://estply.com/kupsiste-poliitika	**83** / 98	**3.90 s** / 681 ms	**0.000** / 0.000

Optimization Checklist

0 of 2 passing — 0 pass · 0 warn · 2 fail · 6 n/a

Item	Status	Detail
Page caching plugin / CDN active	**Fail**	No WordPress cache plugin marker or CDN edge cache detected on the document response.
Response compressed (gzip / brotli)	N/A	Response is not compressed but only 337 bytes — too small to matter.
Images lazy-loaded	N/A	No raster elements found.
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	N/A	No external scripts on the page.

Fixes

Priority 1: Critical

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

1A. Cut mobile LCP from 4.8 s by fixing image delivery `Performance`

- **Impact:** LCP, Speed Index, total page weight
- **Problem:** Mobile LCP is 4.8 s (desktop 2.7 s) and PSI's `image-delivery-insight` estimates 276 KiB of savings; the runtime capture shows 8 image requests totalling 2.70 MB of a 2.76 MB page.
- **Solution:**
  - Serve the hero and below-fold photos as WebP/AVIF — only the hero (`kaasik-kaupo-kalda-360x640.webp`) is currently WebP; the rest are `.jpg` / `.png` .
  - Right-size: the inventory lists 27 distinct srcset widths (100–2560 px); trim the ladder to 4–5 breakpoints so mobile doesn't fetch oversized candidates.
  - Preload the actual LCP image and keep `fetchpriority="high"` on it:

```
<link rel="preload" as="image" href="/wp-
content/uploads/2026/10/hero.webp"
      imagesrcset="..." imagesizes="100vw" fetchpriority="high">
```

  - Re-run PSI to confirm LCP < 2.5 s on mobile.

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

- **Impact:** Lighthouse accessibility (91 mobile), WCAG 2.5.8 / 4.1.2
- **Problem:** PSI mobile accessibility is 91 with `button-name` (score 0.00, weight 10) and `target-size` (score 0.00, weight 7) failing — icon-only controls have no accessible name and are too small to tap.
- **Solution:**
  - Give every icon button an accessible name:

```
<button type="button" aria-label="Ava menüü"><svg aria-
```

```
hidden="true">…</svg></button>
```

- Enforce ≥44×44 px hit areas (WCAG 2.5.8) via padding or `min-width` / `min-height`, plus ≥8 px spacing between adjacent targets.
- Verify with keyboard-only navigation and a screen reader.

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

- **Impact:** CLS, mobile Performance score
- **Problem:** Mobile CLS is 0.491 (desktop 0.138); Lighthouse attributes shift 0.481 to div#page > div.main > div.main__footer > footer.footer.
- **Solution:**
  - Reserve the footer's final height up front: give the footer container a `min-height` matching its rendered height, or render its content server-side instead of injecting it after load.
  - If the shift comes from a late-injected cookie banner or lazyloaded logo, set explicit `width` / `height` on the image and position the banner with `position: fixed` so it does not reflow the document.
  - Re-run Lighthouse mobile after the change and confirm CLS < 0.1.

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

- **Impact:** LCP (3.8 s mobile), Speed Index (3.86 s)
- **Problem:** The optimized-web checklist fails "Hero image eagerly loaded": the hero (uploads/2026/08/6c041c12…png) has loading="lazy" and no fetchpriority, delaying mobile LCP to 3.8 s.
- **Solution:**

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

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

1E. Remove the document redirect and cut server response time `Performance`

- **Impact:** TTFB, FCP, LCP, Speed Index
- **Problem:** The browser runtime shows the non-trailing-slash document taking 1.56 s before the 142 ms canonical response, and PSI's document-latency-insight estimates 1,980 ms of savings.

- **Solution:**
  - Link internally to the canonical trailing-slash URL (`https://estply.com/en/2026/07/06/vineeri-kvaliteediklassid-selgeks/`) so the redirect hop is never paid.
  - Ensure the canonical URL is warmed in the WP Rocket cache after deploy.
  - Verify the redirect is a single 301 at the edge, not a chain through Apache/PHP.

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

- **Impact:** LCP (mobile 3.9 s), Speed Index 2.55 s
- **Problem:** The optimization checklist flags the hero image (…/2026/08/6c041c12fb0c531933532c08c2749a1a836d595a.png) as loading="lazy" with no fetchpriority set, and mobile LCP is 3.9 s versus 0.8 s on desktop.
- **Solution:**
  - Remove `loading="lazy"` from the hero/LCP image and add `fetchpriority="high"` :

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

  - Keep `loading="lazy"` only on below-the-fold images.
  - If the hero is injected by JS or a slider, preload it in `<head>` :

```
<link rel="preload" as="image" href="/wp-
content/uploads/2026/08/hero.png" fetchpriority="high">
```

1G. Stop returning 429 on the privacy policy URL `Performance`

- **Impact:** Availability, TTFB, all downstream audits
- **Problem:** The document returned HTTP 429 with `retry-after: 10` and a 337 B body titled "429 Too Many Requests"; the browser runtime logged "Failed to load resource: the server responded with a status of 429".
- **Solution:**
  - Identify the rate limiter (WAF / ZoneOS / WordPress security plugin) and whitelist the privacy-policy path, or raise the threshold for anonymous GETs.
  - Serve the page from a full-page cache so repeat requests never reach PHP:

```
Cache-Control: public, max-age=600, s-maxage=86400, stale-while-
revalidate=60
```

    - Ensure 429 responses are not cached by the CDN and that `retry-after` is honored by crawlers.

1H. Cut mobile LCP from 3.9 s `Performance`

- **Impact:** LCP, Speed Index, TTI
- **Problem:** Mobile LCP is 3.9 s (desktop 0.8 s) with `render-blocking-insight` estimating 600 ms of savings and `document-latency-insight` 510 ms; Speed Index is 2.87 s on mobile vs 939 ms on desktop.
- **Solution:**
    - Inline critical CSS and defer the rest; move non-critical `<link rel=stylesheet>` out of the critical path.
    - Preload the LCP image and add `fetchpriority="high"`; do not lazy-load it.
    - Flatten the `network-dependency-tree-insight` chain: preconnect to the image/CDN origin and remove serial request waterfalls.
    - Reduce document latency by serving the HTML from cache (see the 429 fix).

1I. Give every button an accessible name `Accessibility`

- **Impact:** WCAG 4.1.2, Lighthouse accessibility score
- **Problem:** Lighthouse fails `button-name` with score 0.00 (weight 10) — buttons on the page have no accessible name, so screen readers announce them as just "button".
- **Solution:**
    - Add visible text or an `aria-label` to each button:

```
<button type="button" aria-label="Ava küpsiste eelistused">…
</button>
```

    - For icon-only buttons, keep the icon `aria-hidden="true"` and put the label on the button.
    - While in this area, verify the 6 color-contrast nodes axe could not determine (gradients/alpha) with a contrast checker at ≥4.5:1.

Priority 2: Important

Essential for compliance, user reach, and search visibility.

2A. Reduce Speed Index (6.01 s mobile) `Performance`

- **Impact:** Speed Index, perceived load
- **Problem:** Mobile Speed Index is 6.01 s versus 1.48 s on desktop, and PSI flags `network-dependency-tree-insight` and `lcp-breakdown-insight` as failing.

- **Solution:**
  - Inline the critical CSS for the above-the-fold hero and defer `global.3578d4f092e5450b.css` (34.3 KB).
  - Preconnect to `https://cdn.jsdelivr.net` (currently only 1 request, 2.7 KB, but it sits on the critical path).
  - Audit the 21 scripts: 2 defer, 0 async — move non-critical WP Rocket / cookie-consent bootstrapping behind `requestIdleCallback`.
  - Check the 3 fonts (`open-sans-semibold.woff2` etc.) for `font-display: swap` and preload the one used above the fold.

2B. Strengthen the Content-Security-Policy `Security`

- **Impact:** XSS defense-in-depth
- **Problem:** CSP is present but only sets `frame-ancestors 'self'` — no `default-src`, no `object-src 'none'`, and no script/resource restrictions, so it provides no XSS mitigation.
- **Solution:** Deploy 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
  ```

  Note: the inferred `hasUserContent` signal comes from an anchor containing "upload" — this looks like a media/uploads path on a manufacturer brochure site, not real UGC, so this is P2 rather than P1. Revisit if a login or user-submitted content is added.

2C. Add a meta description `SEO`

- **Impact:** Search snippet CTR, Lighthouse SEO
- **Problem:** HTML inventory shows `Description: not set` and PSI's `meta-description` audit scores 0.00.
- **Solution:** Add a 140–160 character description in the page head (or via Yoast/RankMath):

  ```
  <meta name="description" content="ESTPLY toodab kvaliteetset kasevineeri Jõgevamaa kaasaegses vineeritehases – usaldusväärne Eesti vineer Lemeks Grupilt.">
  ```

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

- **Impact:** Markup validity, image loading correctness

- **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="auto"` without `loading="lazy"`, and two `srcset` values missing width descriptors.
- **Solution:**
  - Remove `defer` / `async` from WP Rocket's `text/rocketlazyloadscript` data blocks (they are inert data, not executable scripts).
  - Drop the empty `<link data-rocket-prefetch href="" rel="dns-prefetch">` or give it a real origin.
  - Replace `src` with `srcset` on `<source>` elements.
  - Add `loading="lazy"` to the `sizes="auto"` image, or use an explicit `sizes` value.
  - Add width descriptors to the two `srcset` values at lines 794 and 814:

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

2E. Add missing hardening headers and SRI `Security`

- **Impact:** Referrer leakage, feature abuse, cross-origin isolation, supply-chain integrity
- **Problem:** Referrer-Policy, Permissions-Policy, COOP and CORP are all missing; HSTS lacks `preload`; and the single cross-origin script (`cdn.jsdelivr.net/.../iframemanager.js`) has no `integrity` attribute.
- **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 Strict-Transport-Security "max-age=63072000;
includeSubDomains; preload"
```

Add SRI to the jsdelivr tag:

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

Submit the domain at hstspreload.org once the header is live.

2F. Close the two WordPress exposure warnings `Best Practices`

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

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

  - Move or protect the login: add a WAF rule / IP allowlist on `/wp-login.php`, or front it with a custom login slug plugin plus rate limiting and 2FA.

2G. Add a single H1 and a real heading hierarchy `Accessibility`

- **Impact:** Document outline, screen-reader navigation, SEO
- **Problem:** The HTML inventory reports h1 ×0, h2 ×0, h3 ×0, h4 ×0, h5 ×0, h6 ×0, and axe flags page-has-heading-one (moderate).
- **Solution:**
  - Wrap the article title in exactly one `<h1>`.
  - Promote section titles to `<h2>` and sub-sections to `<h3>` in document order.
  - Do not use styled `<div>` / `<p>` for visual headings.

2H. Name icon buttons and enlarge touch targets `Accessibility`

- **Impact:** WCAG 4.1.2 Name/Role/Value, 2.5.8 Target Size
- **Problem:** PSI mobile accessibility fails `button-name` (score 0.00, weight 10) and `target-size` (score 0.00, weight 7).
- **Solution:**
  - Give every button an accessible name: visible text, or `aria-label="Close"` / `<span class="visually-hidden">Close</span>` for icon-only controls.
  - Ensure interactive targets are at least 24×24 CSS px (44×44 recommended) or have ≥24 px spacing:

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

2I. Fix invalid srcset entries missing width descriptors `Best Practices`

- **Impact:** Responsive image selection, W3C validity

- **Problem:** W3C reports 2 errors: srcset values on the two uploads PNGs specify no width while a `sizes` attribute is present (lines 399 and 419).
- **Solution:**

```
<img src="…6c041c12….png"
     srcset="…6c041c12….png 251w"
     sizes="(max-width: 600px) 100vw, 251px"
     width="251" height="134" alt="">
```

  Every candidate in `srcset` must carry a `w` or `x` descriptor when `sizes` is used.

2J. Add Subresource Integrity to the jsDelivr script `Security`

- **Impact:** Supply-chain integrity of third-party JS
- **Problem:** Security basics reports "Subresource Integrity — warn: 1 of 1 cross-origin scripts lack an integrity attribute" (cdn.jsdelivr.net/gh/orestbida/iframemanager@1.3.0).
- **Solution:**

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

  Generate the hash with `openssl dgst -sha384 -binary file.js | openssl base64 -A`. Better still, self-host the file.

2K. Shorten the critical request chain (document latency) `Performance`

- **Impact:** LCP, FCP, Speed Index
- **Problem:** PSI's `document-latency-insight` reports ~840 ms of estimated savings and `network-dependency-tree-insight` fails; the document request itself took 1.23 s in the runtime capture.
- **Solution:**
  - Inline the critical CSS for the above-the-fold region and defer the two external stylesheets (34.6 KB total).
  - Preconnect to `cdn.jsdelivr.net` (already a preconnect hint exists — verify it is on the critical path).
  - Reduce the 23 script tags: audit which WP Rocket–delayed scripts are actually needed on a privacy-policy page and drop the rest.

- Enable full-page cache / CDN edge caching so the HTML is served from cache rather than regenerated per request.

2L. Eliminate forced reflow `Performance`

- **Impact:** LCP, INP, main-thread work
- **Problem:** PSI reports `forced-reflow-insight` failing (score 0.00) on mobile.
- **Solution:**
  - Batch DOM reads before writes; avoid interleaving `offsetWidth` / `getBoundingClientRect()` with style mutations.
  - Defer layout-dependent JS (cookie banner, iframemanager) until after first paint.
  - Profile with DevTools Performance → "Forced reflow" annotations to locate the offending handler.

2M. Allow browser caching of the HTML document `Performance`

- **Impact:** Repeat-visit TTFB, LCP
- **Problem:** The document is served with `cache-control: max-age=0` and an `expires` value equal to the response time, so every navigation revalidates despite WP Rocket being active.
- **Solution:**
  - Serve cached HTML with a short but non-zero TTL and a stale-while-revalidate window:

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

  - Keep `max-age=0` only for logged-in or personalized responses.
  - Verify the CDN/edge layer (ZoneOS) is not overriding the origin's cache headers.

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

- **Impact:** WCAG 4.1.2, 2.5.8; PSI accessibility 91
- **Problem:** Lighthouse flags `button-name` (score 0.00, weight 10) and `target-size` (score 0.00, weight 7) on mobile, even though axe-core reported 0 violations — likely a state (cookie banner / consent dialog) not present during the axe run.
- **Solution:**
  - Add visible text or `aria-label` to every `<button>`, especially in the cookie consent banner:

```
<button type="button" aria-label="Accept all cookies">▫</button>
```

- Ensure interactive targets are at least 24×24 px with adequate spacing (44×44 px recommended):

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

- Re-run axe with the consent banner open to confirm.

2O. Block the WordPress installer and restrict the default login path `Security`

- **Impact:** Attack surface, brute-force exposure
- **Problem:** Security basics reports `/wp-admin/install.php` reachable and the login form served on the default `/wp-login.php` path.
- **Solution:**
  - Block the installer in `.htaccess`:

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

  - Add rate limiting / 2FA on `/wp-login.php`, or move the login behind a custom path or basic-auth gate.
  - Note: the Security basics verdict is PASS, but PASS only means the high-level hygiene checks are in place — it does **not** mean the site is secure.

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

- **Impact:** WCAG 4.1.2, 2.5.8; mobile accessibility score
- **Problem:** PSI mobile accessibility is 91 with `button-name` (score 0.00, weight 10) and `target-size` (score 0.00, weight 7) failing.
- **Solution:**
  - Give every `<button>` visible text or an `aria-label`, e.g. `<button aria-label="Close cookie banner">`.
  - Ensure interactive targets are at least 24×24 px (44×44 recommended) with adequate spacing:

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

2Q. Set an explicit Cache-Control policy `Performance`

- **Impact:** Repeat-visit TTFB, CDN efficiency

- **Problem:** The response has no `cache-control`, `etag`, `last-modified` or `expires` header — the security tool flags "no cache-control header — caching behavior is unpredictable" and the checklist fails "Page caching plugin / CDN active".
- **Solution:**

  ```
  # HTML
  Cache-Control: public, max-age=600, s-maxage=86400
  # Hashed static assets
  Cache-Control: public, max-age=31536000, immutable
  ```

  Enable a WordPress page-cache plugin or CDN edge cache in front of the origin.

2R. Fix document caching and server response latency `Performance`

- **Impact:** TTFB, FCP, repeat-visit performance
- **Problem:** The document is served with `cache-control: max-age=0` and Lighthouse's `document-latency-insight` estimates 1,790 ms of savings; the browser capture shows the HTML document taking 941 ms.
- **Solution:**
  - Let WP Rocket serve a cached HTML copy with a positive TTL, e.g. `Cache-Control: public, max-age=600, s-maxage=3600`.
  - Ensure the page cache is warmed after deploy so the first visitor does not pay the cold-start cost.
  - Investigate the 941 ms document response (PHP/DB work, missing full-page cache hit, or origin latency behind ZoneOS).

2S. Enlarge touch targets to at least 44×44 px `Accessibility`

- **Impact:** WCAG 2.5.8, mobile usability
- **Problem:** Lighthouse fails `target-size` with score 0.00 (weight 7) — interactive elements are too small or too close together for touch.
- **Solution:**
  - Ensure every link/button has a hit area of at least 24×24 CSS px (44×44 recommended):

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

  - Add spacing between adjacent icon links so targets do not overlap.

2T. Fix the 8 W3C validation errors `Best Practices`

- **Impact:** HTML validity, lazy-load correctness
- **Problem:** W3C reports 8 errors: 5 `script type="text/rocketlazyloadscript"` elements carry `defer`, 1 carries `async`, and 2 `srcset` candidates omit a width while `sizes` is present.
- **Solution:**
  - WP Rocket's `text/rocketlazyloadscript` is a data block, so `defer` / `async` are invalid on it. Either let WP Rocket rewrite the type at runtime without those attributes, or exclude those specific scripts from delay:

```
add_filter('rocket_delay_js_exclusions', fn($e) => array_merge($e,
['cookieyes']));
```

  - Fix the two `srcset` entries so every candidate has a width descriptor:

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

Priority 3: Best Practice

Recommended for long-term maintainability.

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

- **Impact:** Rich results eligibility, mobile usability
- **Problem:** PSI's `structuredData` and `tapTargets` audits fail, and the single JSON-LD block is typed `Unknown` in the inventory.
- **Solution:**
  - Replace the untyped JSON-LD with a valid `Organization` / `Manufacturer` schema including `name`, `url`, `logo`, `address` and `sameAs`.
  - Validate at search.google.com/test/rich-results.
  - Enlarge tap targets to ≥44×44 px with adequate spacing (overlaps with the accessibility fix above).

3B. Verify contrast and alt-text on undetermined elements `Accessibility`

- **Impact:** WCAG 1.4.3, 1.1.1
- **Problem:** axe-core returned 0 violations but could not determine contrast on 9 nodes, and the hero image (`kaasik-kaupo-kalda-360x640.webp`) carries an empty `alt=""` despite being the LCP element.
- **Solution:**

- Manually check the 9 undetermined nodes for ≥4.5:1 contrast (3:1 for large text), especially text over gradients or with alpha.
- Confirm the hero's empty `alt` is intentional; if it conveys content, supply descriptive Estonian alt text.
- Disambiguate the repeated link text ("meist" ×2, "tooted" ×2, "kontakt" ×2) with `aria-label` or surrounding context.

3C. Trim technology disclosure and deprecated APIs `Best Practices`

- **Impact:** Fingerprinting surface, Lighthouse Best Practices (81)
- **Problem:** The `Server: Apache / ZoneOS` header discloses the stack, and PSI's `deprecations` audit reports 1 deprecated API warning.
- **Solution:**
  - Suppress the version/OS detail:

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

  - Identify the deprecated API in the Lighthouse `deprecations` audit and replace it (commonly `document.write` or a legacy `XMLHttpRequest` sync call).

3D. Tighten 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 no script or resource restrictions apply. Site signals show no auth, payments, user content or commerce, so this is a hardening item rather than an urgent one.
- **Solution:** Add a nonce-based policy rather than a flat allowlist:

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

  Roll out in report-only mode first to catch breakage from WP Rocket's lazyload rewriting.

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

- **Impact:** Information leakage, feature abuse, origin isolation

- **Problem:** Security basics marks Referrer-Policy, Permissions-Policy, Cross-Origin-Opener-Policy and Cross-Origin-Resource-Policy as fail (all missing from the response headers).
- **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-site
```

3F. Fix WP Rocket lazyload script markup rejected by the validator `Best Practices`

- **Impact:** W3C validity (6 of 8 errors)
- **Problem:** W3C reports 5 errors for `type="text/rocketlazyloadscript"` with `defer` and 1 with `async` — data-block scripts must not carry those attributes.
- **Solution:**
  - Update WP Rocket to the current release, which emits valid lazyload markup.
  - If it persists, exclude the affected scripts from Delay JS execution in WP Rocket → File Optimization → Delay JavaScript execution, so they render as normal `<script defer src=…>`.

3G. Stop sending cache-control: max-age=0 on the document `Performance`

- **Impact:** Repeat-visit TTFB, back/forward navigation
- **Problem:** The document response carries `cache-control: max-age=0` with an `expires` timestamp in the past, despite WP Rocket being active.
- **Solution:**
  - In WP Rocket → Cache → Browser cache, enable HTML browser caching with a short TTL (e.g. 600 s) and rely on the `last-modified` validator for revalidation.
  - Confirm the edge/CDN is not overriding the origin's Cache-Control.

3H. Fix structured data and vague repeated link text `SEO`

- **Impact:** Rich results eligibility, link-purpose clarity
- **Problem:** PSI fails the `structuredData` audit and the JSON-LD block's type is reported as "Unknown"; the inventory also lists repeated vague anchors ("about us" ×2, "products" ×2, "resources" ×2, "contact" ×2).
- **Solution:**

- Validate the JSON-LD at validator.schema.org and declare an explicit `@type` (e.g. `Article` with `headline`, `datePublished`, `author`, `image`).
- Disambiguate repeated anchors with `aria-label` or surrounding context, e.g. `<a href="/en/about/">About estply</a>`.

3I. Harden the WordPress surface `Security`

- **Impact:** Brute-force and takeover exposure
- **Problem:** Security basics warns that `/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 endpoint (custom path, HTTP auth on `/wp-login.php`, or a login-limiter plugin).
  - Also strip the `Server: Apache / ZoneOS` banner via `ServerTokens Prod` / `ServerSignature Off`.

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

- **Impact:** XSS defense-in-depth
- **Problem:** The CSP is `frame-ancestors 'self'` only — no `default-src`, no `object-src 'none'`, and no script/resource restrictions. Site signals show no auth, payments or user content, so this is a P3 hardening item rather than an urgent fix.
- **Solution:** Deploy a nonce-based policy rather than a flat allowlist:

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

  - Roll out in `Content-Security-Policy-Report-Only` first and fix violations before enforcing.
  - WP Rocket's `text/rocketlazyloadscript` placeholders will need nonce propagation.

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

- **Impact:** Privacy leakage, origin isolation, HSTS coverage

- **Problem:** All five are missing or incomplete: `referrer-policy`, `permissions-policy`, `cross-origin-opener-policy`, `cross-origin-resource-policy` are absent, and HSTS (`max-age=31536000; includeSubDomains`) lacks `preload`.
- **Solution:**

```
Referrer-Policy: strict-origin-when-cross-origin
Permissions-Policy: camera=(), microphone=(), geolocation=(),
payment=()
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-site
Strict-Transport-Security: max-age=63072000; includeSubDomains;
preload
```

  Only submit to the preload list once you are confident every subdomain is HTTPS-only.

3L. Add Subresource Integrity to the jsDelivr script `Security`

- **Impact:** Supply-chain tampering risk
- **Problem:** Security basics reports 1 of 1 cross-origin scripts lacks an `integrity` attribute — `iframemanager.js` from `cdn.jsdelivr.net`.
- **Solution:**

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

  Generate the hash from the exact pinned version and update it whenever the version changes.

3M. Fix invalid srcset width descriptors `Best Practices`

- **Impact:** Responsive image selection, HTML validity
- **Problem:** W3C reports 2 errors: `srcset` on the two `<img>` elements specifies no width descriptor while `sizes` is present (lines 536 and 556).
- **Solution:**

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

  Every candidate in `srcset` must carry a `w` descriptor when `sizes` is used.

3N. Replace vague "here" link text `SEO`

- **Impact:** SEO 85, link-text audit, screen-reader clarity
- **Problem:** PSI's `link-text` audit fails with 2 links lacking descriptive text, and the inventory lists "here" ×2 among repeated vague anchors.
- **Solution:**
  - Rewrite the anchor text to describe the destination, e.g. "read our cookie policy" instead of "here".
  - If the visual design requires short text, add `aria-label`:

```
<a href="/en/cookies" aria-label="Read our cookie policy">here</a>
```

3O. Add structured data `SEO`

- **Impact:** SEO 85, rich-result eligibility
- **Problem:** PSI's `structured-data` audit fails, and the single JSON-LD block on the page has an unrecognized type.
- **Solution:**
  - Add `WebPage` / `Organization` JSON-LD with `@type`, `name`, `url` and `inLanguage` matching the `en` / `et` hreflang pair.
  - Validate with the Rich Results Test and Schema Markup Validator.

3P. Suppress the Server header `Security`

- **Impact:** Technology disclosure
- **Problem:** The response discloses `Server: Apache / ZoneOS`, and Security basics flags technology disclosure as a warn.
- **Solution:**

```
ServerTokens Prod
ServerSignature Off
Header unset Server
```

  If the edge (ZoneOS) sets the header, strip it at the CDN layer instead.

3Q. Add remaining hardening headers `Security`

- **Impact:** Privacy leakage, feature abuse, origin isolation
- **Problem:** `referrer-policy`, `permissions-policy`, `cross-origin-opener-policy` and `cross-origin-resource-policy` are all missing; HSTS lacks `preload`; the `server` header discloses `Apache / ZoneOS`.
- **Solution:**

```
Header always set Referrer-Policy "strict-origin-when-cross-origin"
Header always set Permissions-Policy "geolocation=(), camera=(),
microphone=()"
Header always set Cross-Origin-Opener-Policy "same-origin"
Header always set Cross-Origin-Resource-Policy "same-origin"
Header always set Strict-Transport-Security "max-age=31536000;
includeSubDomains; preload"
ServerTokens Prod
ServerSignature Off
```

Submit the domain to hstspreload.org once the preload directive is live.

3R. Fix the 8 W3C validation errors `Best Practices`

- **Impact:** Markup validity, lazy-load correctness
- **Problem:** W3C reports 8 errors: 5× `defer` and 1× `async` on `type="text/rocketlazyloadscript"` data-block scripts, plus 2× `srcset` candidates missing a width descriptor while `sizes` is present.
- **Solution:**
  - WP Rocket's `text/rocketlazyloadscript` is a data block, so `defer` / `async` are invalid there — let the plugin rewrite the type at runtime instead of hard-coding the attributes.
  - Add width descriptors to every `srcset` candidate:

```
<img src=".../a.png" sizes="(max-width: 768px) 100vw, 600px"
     srcset=".../a-300.png 300w, .../a-600.png 600w" alt="">
```

3S. Re-verify lang and landmarks on the real page `Accessibility`

- **Impact:** WCAG 3.1.1, 1.3.1
- **Problem:** axe reports `html-has-lang` (serious), `landmark-one-main` and `region`, and the inventory shows no `<nav>`, `<main>`, `<header>` or `<footer>` — but these were captured on the 429 error page, so they may not reflect the real document.
- **Solution:**
  - Re-run axe against the live page once the 429 is resolved.
  - Regardless, ensure the error template itself is valid: `<html lang="et">`, a single `<main>`, and all content inside landmarks.
  - Add a skip link: `<a href="#main" class="skip-link">Otse sisu juurde</a>`.

3T. Add the remaining low-cost security headers `Security`

- **Impact:** Referrer leakage, feature abuse, cross-origin isolation
- **Problem:** Referrer-Policy, Permissions-Policy, Cross-Origin-Opener-Policy and Cross-Origin-Resource-Policy are all missing, HSTS lacks `preload`, and the jsdelivr script has no `integrity` attribute.
- **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 Strict-Transport-Security "max-age=31536000;
includeSubDomains; preload"
```

  - Add SRI to the jsdelivr iframemanager script, or self-host it.
  - Consider trimming the `Server: Apache / ZoneOS` header.

3U. Close WordPress hardening gaps `Best Practices`

- **Impact:** Attack surface, brute-force exposure
- **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>
```

  - Move the login to a custom path or put `/wp-login.php` behind rate limiting / a WAF rule.

3V. Declare a structured-data type and disambiguate repeated link text `SEO`

- **Impact:** Rich results eligibility, link context
- **Problem:** The single JSON-LD block parses as type "Unknown" and PSI fails `structuredData`; the page also repeats vague anchors ("meist" ×2, "tooted" ×2, "kontakt" ×2).
- **Solution:**
  - Emit a concrete schema type, e.g. `WebPage` with `inLanguage: "et"` and a `@id` matching the canonical URL.
  - Where repeated anchors appear in different contexts, add `aria-label` or surrounding text so each link's destination is clear out of context.