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/en/kupsiste-poliitika
- https://estply.com/kupsiste-poliitika
- https://estply.com/kontakt

Summary of results

Overall Score: 68 / 100
Status: Needs Improvement

Site overall 68 is the mean of 5 pages. Scores range 63 (https://estply.com/) → 75 (https://estply.com/kontakt). Weakest page: Mobile PSI performance is 64 against 92 on desktop, driven by a 7.0 s mobile LCP and 8.2 s Speed Index while desktop LCP is 1.5 s — a divergence that points at mobile image delivery rather than server speed (TTFB 41 ms, TBT 0 ms, CLS 0.006). The page ships 963.5 KB, of which 766.4 KB is images, including a single 464.4 KB hero WebP; Lighthouse estimates 544 KiB of image-delivery savings and 270 ms from font-display. Accessibility is the strongest area (axe 0 violations, PSI 91 mobile / 96 desktop), though PSI still flags unnamed buttons and undersized tap targets and axe left 17 contrast nodes undetermined. Security basics FAILED — HSTS, X-Frame-Options and X-Content-Type-Options are all missing — and the document is served with cache-control max-age=0 despite WP Rocket being active. SEO sits at 92 with no meta description, and 32 console errors from a cross-origin SVG on rocketcdn.me add runtime noise.

Per-page scores

 Needs Improvement · https://estply.com/

Score	Performance	Accessibility	Best Practices	SEO	Security
63	64	91	96	92	FAILED

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

Score	Performance	Accessibility	Best Practices	SEO	Security
66	66	91	100	100	FAILED

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

Score	Performance	Accessibility	Best Practices	SEO	Security
64	72	91	100	85	FAILED

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

Score	Performance	Accessibility	Best Practices	SEO	Security
70	72	91	100	92	FAILED

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

Score	Performance	Accessibility	Best Practices	SEO	Security
75	82	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/	**64** / 92	**7.02 s** / 1.54 s	**0.006** / 0.001
https://estply.com/en/2026/07/06/vineeri-kvaliteediklassid-selgeks	**66** / 94	**3.74 s** / 833 ms	**0.491** / 0.133
https://estply.com/en/kupsiste-poliitika	**72** / 93	**4.55 s** / 955 ms	0.000 / **0.001**
https://estply.com/kupsiste-poliitika	**72** / 93	**4.54 s** / 970 ms	0.000 / **0.001**

URL	Performance (M / D)	LCP (M / D)	CLS (M / D)
https://estply.com/kontakt	**82** / 98	**3.92 s** / 927 ms	**0.014** / 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.
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. Fix the 7.0 s mobile LCP on the hero image `Performance`

- **Impact:** LCP, Speed Index, FCP
- **Problem:** Mobile LCP is 7.0 s versus 1.5 s on desktop, and the hero request kaasik-kaupo-kalda-1600x900.webp is 464.4 KB — the largest single resource on the page.
- **Solution:**
  - Preload the hero and give it priority:

```
<link rel="preload" as="image" href="/…/kaasik-kaupo-kalda-
1600x900.webp"
      imagesrcset="/…/kaasik-kaupo-kalda-640.webp 640w, /…/kaasik-
kaupo-kalda-1024.webp 1024w, /…/kaasik-kaupo-kalda-1600.webp 1600w"
      imagesizes="100vw" fetchpriority="high">
```

  - Add `fetchpriority="high"` to the hero `<img>` (currently not set).
  - Re-encode the 1600×900 hero to AVIF/WebP at ~120–180 KB; 464 KB is far above what a hero needs.
  - Verify the `sizes` attribute matches the real rendered width so mobile does not download the 1600w candidate.

1B. Cut image payload (766 KB of a 963 KB page) `Performance`

- **Impact:** LCP, Speed Index, total page weight
- **Problem:** Browser runtime shows 766.4 KB of images out of 963.5 KB total, and Lighthouse's image-delivery-insight estimates 544 KiB of savings.
- **Solution:**
  - Re-encode the remaining JPEGs (`kaupokalda-com-dji_…-594x396.jpg` 49.7 KB, `dsc_5118-324x216.jpg` , `estply-cta-1-520x140.jpg`) to WebP/AVIF.
  - The inventory lists 28 distinct srcset widths (100→3200) — trim to 4–5 breakpoints per image so the browser picks a sane candidate.
  - Fix the two `srcset` entries that omit width descriptors (W3C errors at lines 776 and 796) so candidate selection actually works.
  - Lazy-load the one remaining below-the-fold image that lacks `loading="lazy"` .

1C. 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/frame-ancestors and X-Content-Type-Options are all absent from the response.
- **Solution:** Send from the origin (Apache syntax):

  ```
  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 to hstspreload.org once the max-age is stable.

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

- **Impact:** CLS, mobile Performance score
- **Problem:** Mobile CLS is 0.491 (desktop 0.133) with the dominant shift attributed to `div#page > div.main > div.main__footer > footer.footer` at 0.481.
- **Solution:** Reserve space for whatever the footer injects after load (cookie banner, iframe manager, or late-loading widget):
  - Give the footer container a fixed `min-height` matching its rendered height.
  - If a consent banner or iframe is inserted into the footer, render a placeholder with the same dimensions server-side instead of injecting it post-load.
  - Avoid `position: sticky` / `fixed` footer elements that reflow the document on hydration.
  - Re-run Lighthouse after each change to confirm CLS < 0.1.

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

- **Impact:** LCP, FCP
- **Problem:** The hero image (`uploads/2026/08/6c041c12fb0c531933532c08c2749a1a836d595a.png`) carries `loading="lazy"` and no `fetchpriority`, and mobile LCP is 3.7 s.
- **Solution:**

  ```
  <img src="/wp-
  content/uploads/2026/08/6c041c12fb0c531933532c08c2749a1a836d595a.pn
  g"
       alt="..." width="251" height="134"
       loading="eager" fetchpriority="high" decoding="async">
  ```

Also add a `<link rel="preload" as="image" fetchpriority="high">` for the same URL in `<head>`.

1F. 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 and CSP frame-ancestors are missing.
- **Solution:** Send from the origin (Apache syntax):

```
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 Content-Security-Policy "frame-ancestors 'self'"
```

Verify preload eligibility at hstspreload.org after deploy.

1G. Cut document latency and render-blocking CSS `Performance`

- **Impact:** FCP, Speed Index, LCP
- **Problem:** FCP is 3.04 s and Speed Index 7.35 s on mobile; the document request took 1.37 s and PSI's document-latency-insight estimates 3,250 ms of savings, with 4 external stylesheets plus 3 inline blocks (9.6 KB) in the critical path.
- **Solution:**
  - Enable full-page caching / CDN edge caching for this static policy page (WP Rocket is present but the document still returns `cache-control: max-age=0`).
  - Inline critical above-the-fold CSS and defer the rest:

```
<link rel="preload" href="/wp-content/themes/wordpress-
base/…/style.css" as="style" onload="this.rel='stylesheet'">
```

  - Reduce the 78.4 KB decoded HTML (79 KB document) by trimming inline markup and unused inline CSS.

1H. Add baseline security headers (HSTS, nosniff, frame-ancestors) `Security`

- **Impact:** Transport security, clickjacking, MIME sniffing
- **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:** Send from the origin (Apache shown in the Server header):

```
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 Content-Security-Policy "frame-ancestors 'self'"
```

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

1I. 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 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 — the two tools disagree on these elements.
- **Solution:**
  - Add visible text or `aria-label` to every `<button>`, e.g. `<button aria-label="Close cookie banner">`.
  - Ensure interactive controls are at least 24×24 px (44×44 recommended) with adequate spacing:

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

  - Re-run axe with the same viewport as Lighthouse to reconcile the discrepancy.

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

- **Impact:** LCP, Speed Index, FCP
- **Problem:** The hero PNG (uploads/2026/08/6c041c12…png) is served with loading="lazy" and no fetchpriority, and mobile LCP is 4.5 s vs 1.0 s on desktop.
- **Solution:**
  - Remove `loading="lazy"` from the hero and add `fetchpriority="high"`:

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

  - Preload it in `<head>`:

```
<link rel="preload" as="image" href="/wp-
content/uploads/2026/08/6c041c12….png" fetchpriority="high">
```

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

1K. Add HSTS, X-Frame-Options and 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 from the response.
- **Solution:** Send from the origin (Apache shown, since `server: Apache / ZoneOS`):

```
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"
```

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

1L. Eager-load the hero image with fetchpriority="high" `Performance`

- **Impact:** LCP, FCP, Speed Index
- **Problem:** The hero image (cz5i9178-100x100.webp) is served with `loading="lazy"` and no `fetchpriority`; mobile LCP is 3.9 s vs 0.9 s on desktop and `lcp-discovery-insight` scores 0.
- **Solution:**
  - Remove `loading="lazy"` from the hero (or set `loading="eager"`).
  - Add `fetchpriority="high"` and preload it:

```
<img src="/wp-content/uploads/2026/10/cz5i9178.webp"
     srcset="… 400w, … 800w, … 1200w" sizes="100vw"
     width="1200" height="600" alt="…"
     loading="eager" fetchpriority="high" decoding="async">
<link rel="preload" as="image" href="/wp-
content/uploads/2026/10/cz5i9178.webp"
      imagesrcset="… 400w, … 800w, … 1200w" imagesizes="100vw"
fetchpriority="high">
```

  - Keep `loading="lazy"` on the 21 below-the-fold images (already correct).

1M. Add baseline security headers (HSTS, X-Frame-Options/frame-ancestors, 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, so the page can be framed and HTTPS downgrade is not enforced.
- **Solution:** Send from the origin (Apache shown):

```
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"
```

Prefer `Content-Security-Policy: frame-ancestors 'self'` once CSP is in place; keep X-Frame-Options as a fallback for older browsers. Verify preload eligibility at hstspreload.org.

Priority 2: Important

Essential for compliance, user reach, and search visibility.

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

- **Impact:** TTFB on repeat views, Speed Index
- **Problem:** The document response carries `cache-control: max-age=0` with no ETag, so every navigation revalidates the full 531,748-byte HTML document even though WP Rocket is active.
- **Solution:**
  - Enable WP Rocket's page cache for anonymous visitors and let it emit a positive `max-age` plus `s-maxage`.
  - Add an ETag or rely on `Last-Modified` for conditional requests.
  - Exclude cart/checkout/logged-in states from the cache rather than disabling it globally.

2B. Reduce the 531 KB HTML document and fix font loading `Performance`

- **Impact:** FCP, Speed Index, render time
- **Problem:** HTML bytes are 531,748 (88 KB gzipped) and Lighthouse's font-display-insight estimates 270 ms of savings from 3 font files totalling 161.4 KB.
- **Solution:**
  - Audit the 531 KB of markup: inline SVG sprites, base64 data URIs and inline styles (9.6 KB across 3 blocks) are the usual culprits — move the sprite to an external file.
  - Add `font-display: swap` (or `optional`) to the Open Sans faces and preload only the regular weight:

```
<link rel="preload" href="/…/open-sans-regular.woff2" as="font"
type="font/woff2" crossorigin>
```

    - Consider self-hosting the two Google Fonts files (47.2 KB from fonts.gstatic.com) to remove a third-party round trip.

2C. Name the buttons and enlarge touch targets `Accessibility`

- **Impact:** WCAG 4.1.2, 2.5.8; PSI accessibility 91
- **Problem:** PSI mobile accessibility is 91 with `button-name` (score 0.00, weight 10) and `target-size` (score 0.00, weight 7) failing; axe reported 0 violations but left 17 color-contrast nodes undetermined.
- **Solution:**
    - Give every `<button>` visible text or an `aria-label`, e.g. `<button aria-label="Open menu">`.
    - Ensure interactive targets are at least 44×44 px with adequate spacing.
    - Manually check the 17 contrast nodes axe could not resolve (gradients/alpha) against 4.5:1 for body text.

2D. Fix the cross-origin SVG that throws 32 console errors `Best Practices`

- **Impact:** Console errors, failed requests, Best Practices score
- **Problem:** The runtime capture logged 32 console events and 31 failed requests, all `Unsafe attempt to load URL …/theme/svg/global.f0c272df5a4f94d0b14a.svg from frame with URL https://estply.com/. Domains, protocols and ports must match.`
- **Solution:**
    - The SVG sprite is being fetched from `27c41eda.delivery.rocketcdn.me` into a same-origin frame context. Serve the sprite from `https://estply.com/...` (exclude it from the RocketCDN rewrite) or inline it once.
    - Alternatively add `crossorigin` to the referencing element and ensure the CDN returns `Access-Control-Allow-Origin`.
    - Re-run the runtime capture to confirm the console is clean.

2E. Add a meta description `SEO`

- **Impact:** SEO score, SERP snippet
- **Problem:** The document has no meta description (`meta-description` audit scores 0.00) and the HTML inventory confirms `Description: not set`, despite a 92 SEO score otherwise.
- **Solution:** Add a 140–160 character description in the page head or via the SEO plugin:

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

```
koosseisus.">
```

Provide a separate English description for the `/en/` hreflang variant.

2F. Add a Content-Security-Policy `Security`

- **Impact:** XSS defense-in-depth
- **Problem:** CSP is missing entirely. The inferred `hasUserContent` signal is a false positive (it fired on an anchor href containing "upload" on a plywood-manufacturer brochure site), but this is WordPress with `/wp-login.php` and `/wp-admin/install.php` reachable, so plugin-borne XSS is a realistic vector.
- **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'
```

Roll it out in report-only mode first — the page loads scripts from cdn.jsdelivr.net and rocketcdn.me, which will need to be accounted for.

2G. Add a heading structure and accessible names for buttons and touch targets `Accessibility`

- **Impact:** WCAG 1.3.1, 2.4.4, 2.5.8; screen-reader navigation
- **Problem:** The heading outline contains 0 h1 and 0 h2–h6, axe flags `page-has-heading-one`, and PSI fails `button-name` (weight 10) and `target-size` (weight 7).
- **Solution:**
  - Wrap the article title in a single `<h1>` and section titles in `<h2>` / `<h3>` in document order.
  - Give every icon-only button an accessible name: `<button aria-label="Close">…</button>`.
  - Enlarge interactive controls to at least 44×44 px with ≥8 px spacing (WCAG 2.5.8).

2H. Enable browser caching for the HTML document `Performance`

- **Impact:** Repeat-visit TTFB, LCP
- **Problem:** The document is served with `cache-control: max-age=0` and an `expires` value one second in the future, forcing revalidation on every navigation.
- **Solution:** Set a short but non-zero document cache with revalidation:

```
Header set Cache-Control "public, max-age=600, s-maxage=3600,
stale-while-revalidate=86400"
```

Keep long-lived immutable caching for hashed static assets (`/wp-content/themes/.../js/*.js`).

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

- **Impact:** HTML validity, script execution order
- **Problem:** W3C reports 7 errors: 5× `defer` on a `type="text/rocketlazyloadscript"` data block (first at line 21) and 2× srcset candidates missing a width descriptor while `sizes` is present (lines 391, 411).
- **Solution:**
  - Remove `defer` from the Rocket Loader data-block script, or move the attribute onto the real script tag it later creates.
  - Add width descriptors to every srcset candidate:

```
<img src="...png" srcset="...png 251w" sizes="251px" width="251"
height="134" alt="">
```

2J. Harden the WordPress install surface `Security`

- **Impact:** Brute-force and takeover risk
- **Problem:** `/wp-admin/install.php` is reachable and the login form is served on the default `/wp-login.php` path; 1 of 1 cross-origin scripts (cdn.jsdelivr) lacks an `integrity` attribute.
- **Solution:**

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

  - Move or protect the login: restrict `/wp-login.php` by IP or add a custom login slug plus rate limiting / 2FA.
  - Add SRI to the jsDelivr script: `<script src="..." integrity="sha384-..." crossorigin="anonymous" defer></script>` .

2K. Enable browser caching for the document `Performance`

- **Impact:** Repeat-visit TTFB, LCP
- **Problem:** The response sends `cache-control: max-age=0` with an `expires` value one second after the request, so every visit revalidates the 78.4 KB document.

- **Solution:**
  - Serve the HTML with a short but non-zero TTL and a validator:

```
Cache-Control: public, max-age=600, s-maxage=3600, stale-while-revalidate=86400
```

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

2L. Self-host fonts and set font-display `Performance`

- **Impact:** FCP, LCP, render-blocking
- **Problem:** 4 font files from fonts.gstatic.com total 96.2 KB (the single largest resource type on the page), the Google Fonts CSS request took 738 ms, and `font-display-insight` is flagged.
- **Solution:**
  - Self-host Open Sans as WOFF2 with `font-display: swap` and preload the one weight used above the fold:

```
<link rel="preload" href="/fonts/open-sans-400.woff2" as="font" type="font/woff2" crossorigin>
```

  - Drop unused weights (400i, 600, 700i) — the page currently requests four variants.

2M. Fix W3C validation errors `Best Practices`

- **Impact:** HTML validity, lazy-load behavior
- **Problem:** W3C reports 7 errors: 5× a `script` data block (`type="text/rocketlazyloadscript"`) carrying a `defer` attribute, and 2× `srcset` candidates missing a width descriptor while `sizes` is present.
- **Solution:**
  - Remove `defer` from the Rocket Loader data-block scripts, or move the attribute into the rewritten tag:

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

  - Add width descriptors to every `srcset` candidate:

```
<img srcset="/img/a-251w.png 251w, /img/a-502w.png 502w" sizes="251px" width="251" height="134" alt="">
```

2N. Harden the WordPress admin surface `Security`

- **Impact:** Brute force, takeover risk
- **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>
```

  - Move or protect the login path (custom login slug plugin, or IP allowlist / basic auth on `/wp-login.php`), and add rate limiting plus 2FA.

2O. Fix heading structure and vague link text `SEO`

- **Impact:** Document outline, link purpose
- **Problem:** The page has 2 `<h1>` elements ("Küpsiste poliitika" and "Privacy Policy") and repeated vague link text such as "here" ×2 and "code of conduct" ×3.
- **Solution:**
  - Keep a single `<h1>` per page; demote the second to `<h2>` or remove it.
  - Replace "here" links with descriptive text, or add `aria-label`:

```
<a href="/en/code-of-conduct" aria-label="Read the Estply code of
conduct">code of conduct</a>
```

2P. Self-host and preload web fonts, trim the font payload `Performance`

- **Impact:** FCP, LCP, Speed Index
- **Problem:** 4 font files from fonts.gstatic.com total 96.2 KB and the fonts.googleapis.com CSS request is the slowest on the page at 1.45 s; Lighthouse flags font-display-insight (est. 60 ms savings).
- **Solution:**
  - Self-host the Open Sans woff2 subsets and drop the `subset=cyrillic` request if unused.
  - Preload the one weight used above the fold:

```
<link rel="preload" as="font" type="font/woff2"
      href="/fonts/open-sans-400.woff2" crossorigin>
```

  - Use `font-display: swap` and `size-adjust` /fallback metrics to avoid layout shift.

2Q. Fix document caching and document latency `Performance`

- **Impact:** TTFB, FCP, LCP
- **Problem:** The document is served with `cache-control: max-age=0` and Lighthouse's document-latency-insight estimates 2,600 ms of savings; the browser runtime shows two document requests at 876 ms and 819 ms.
- **Solution:**
  - Let WP Rocket serve a real cache lifetime for anonymous visitors instead of `max-age=0`:

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

  - Ensure the canonical URL `https://estply.com/kupsiste-poliitika/` is warmed after deploy so the first visitor does not pay the cold-start cost.
  - Investigate the duplicate document request (trailing-slash redirect) shown in the network capture.

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

- **Impact:** WCAG 4.1.2 name/role/value, 2.5.8 target size
- **Problem:** Lighthouse accessibility is 91 mobile / 96 desktop with `button-name` (score 0.00, weight 10) and `target-size` (score 0.00, weight 7) failing, even though axe reported 0 violations.
- **Solution:**
  - Give every icon-only button an accessible name:

```
<button type="button" aria-label="Sulge küpsiste teade">…</button>
```

  - Ensure interactive targets are at least 44×44 px with adequate spacing:

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

  - Manually verify the 8 color-contrast nodes axe could not determine (alpha/gradient backgrounds).

2S. Self-host and preload the Google Fonts `Performance`

- **Impact:** FCP, LCP, render-blocking chain
- **Problem:** The Google Fonts CSS request takes 797 ms and the woff2 file is 47.2 KB from fonts.gstatic.com; `font-display-insight` estimates 120 ms savings and `document-latency-insight` 690 ms.

- **Solution:**
  - Download the Open Sans woff2 subsets and serve them from the same origin.
  - Preload the one weight used above the fold:

```
<link rel="preload" href="/fonts/open-sans-400.woff2" as="font"
type="font/woff2" crossorigin>
```

  - Use `font-display: swap` and drop the unused 400i/700i variants.
  - Remove the fonts.googleapis.com / fonts.gstatic.com third-party origins entirely.

2T. Cache the HTML document `Performance`

- **Impact:** Repeat-view TTFB, navigation speed
- **Problem:** The document is served with `cache-control: max-age=0` even though WP Rocket 3.23.5.1 is active, so every navigation revalidates the 173 KB HTML payload.
- **Solution:**
  - Let WP Rocket serve cached HTML with a short browser TTL plus revalidation:

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

  - Keep `max-age=0` only for logged-in / form-submission responses.
  - Confirm the contact-form POST response is excluded from the page cache.

2U. Deploy a strict nonce-based CSP `Security`

- **Impact:** XSS defense-in-depth
- **Problem:** Content-Security-Policy is missing. Site signals flag user content because of a `<textarea>` in the contact form — that is a submitted form field rather than persisted public content, so this is rated P2 instead of P1, but a WordPress site with a public form still benefits.
- **Solution:** Use nonce + `'strict-dynamic'` rather than a flat allowlist:

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

  Roll out in report-only mode first (`Content-Security-Policy-Report-Only`) to catch inline snippets from WP Rocket and the cookie banner.

2V. Fix the 17 W3C HTML errors `Best Practices`

- **Impact:** Markup validity, parser robustness
- **Problem:** W3C reports 17 errors: 12× `<script type="text/rocketlazyloadscript" … defer>` (invalid data-block type with defer), 2× `srcset` candidates without width descriptors, 1× charset meta after the first 1024 bytes, 2× hidden input with `autocomplete`.
- **Solution:**
  - Move `<meta charset="utf-8">` into the first 1024 bytes of `<head>`.
  - Stop WP Rocket from emitting `defer` on `type="text/rocketlazyloadscript"` scripts (exclude those handles from Delay JS execution), or switch to native `defer` on real `type="text/javascript"` scripts.
  - Add width descriptors to the two offending `srcset` values:

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

  - Remove `autocomplete` from `type="hidden"` inputs (Gravity Forms `gform_hidden` fields).

Priority 3: Best Practice

Recommended for long-term maintainability.

3A. Clear the 8 W3C validation errors `Best Practices`

- **Impact:** Markup validity, image candidate selection
- **Problem:** W3C reports 8 errors: 5× `defer` on `type="text/rocketlazyloadscript"` data blocks, 1× `sizes="auto"` on an eagerly-loaded image, and 2× `srcset` candidates with no width descriptor.
- **Solution:**
  - Drop `defer` from the RocketLazyload data-block scripts (they are not executable JS).
  - Either add `loading="lazy"` to the image using `sizes="auto"` or replace `auto` with an explicit size list.
  - Add width descriptors to the two offending `srcset` values:

```
<img srcset="…6c041c12….png 251w, …6c041c12…@2x.png 502w" sizes="251px" …>
```

3B. Remaining header and WordPress hardening `Security`

- **Impact:** Information disclosure, referrer leakage, supply-chain integrity

- **Problem:** Referrer-Policy, Permissions-Policy, COOP and CORP are all missing; 2 of 2 cross-origin scripts lack SRI; the `Server: Apache / ZoneOS` header discloses the stack; `/wp-admin/install.php` is reachable and login sits on the default `/wp-login.php`.
- **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 unset Server
```

  - Add `integrity` + `crossorigin` to the jsDelivr iframemanager script.
  - Block `/wp-admin/install.php` and `/wp-login.php` at the edge or via `.htaccess` IP allowlist.

3C. Fix structured data and vague anchor text `SEO`

- **Impact:** Rich results eligibility, link context
- **Problem:** The single JSON-LD block parses but its type is reported as `Unknown`, and 8 anchor texts repeat verbatim ("käitumiskoodeks" ×3, "meist" ×2, "tooted" ×2, "kontakt" ×2).
- **Solution:**
  - Replace the JSON-LD with a typed `Organization` + `WebSite` graph so search engines can classify it.
  - Disambiguate repeated links with `aria-label` or visually-hidden suffixes, e.g. `<a href="/meist/">meist<span class="sr-only"> – ESTPLY ettevõttest</span></a>`.

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

- **Impact:** XSS defense-in-depth
- **Problem:** CSP 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 + `'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'
```

Roll it out in report-only mode first to catch breakage from the WP Rocket and iframemanager scripts.

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

- **Impact:** Information leakage, origin isolation
- **Problem:** Referrer-Policy, Permissions-Policy, Cross-Origin-Opener-Policy and Cross-Origin-Resource-Policy are all missing, and the `Server: Apache / ZoneOS` header discloses the stack.
- **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-site"
Header unset Server
```

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

- **Impact:** Rich results, anchor-text relevance
- **Problem:** PSI's modeled `structuredData` audit fails and the JSON-LD block is typed `Unknown`; 7 link texts repeat verbatim (e.g. "code of conduct" ×3, "about us" ×2).
- **Solution:**
  - Emit `Article` / `BlogPosting` JSON-LD with `headline`, `datePublished`, `author`, and `image` for this post.
  - Differentiate repeated anchors with `aria-label` or surrounding context, e.g. `<a href="/en/about/" aria-label="About estply">about us</a>`.

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

- **Impact:** Information leakage, cross-origin isolation, supply-chain integrity
- **Problem:** Referrer-Policy, Permissions-Policy, Cross-Origin-Opener-Policy and Cross-Origin-Resource-Policy are all missing, and 1 of 1 cross-origin scripts (cdn.jsdelivr.net) lacks an `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"
```

Add SRI to the jsDelivr script:

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

3H. Reduce server technology disclosure and validate structured data `Best Practices`

- **Impact:** Fingerprinting surface, rich-result eligibility
- **Problem:** The `Server: Apache / ZoneOS` header discloses the stack, and the single JSON-LD block is typed "Unknown" so it likely does not produce a valid schema.org entity.
- **Solution:**
  - Strip or genericize the Server header at the edge (`ServerTokens Prod` , `ServerSignature Off`).
  - Replace the JSON-LD with a concrete schema.org type, e.g.:

```
{"@context":"https://schema.org","@type":"WebPage","name":"Cookie
policy","url":"https://estply.com/en/kupsiste-poliitika/"}
```

3I. Use one h1 and descriptive link text `Accessibility`

- **Impact:** Document outline, WCAG 2.4.4 link purpose
- **Problem:** The page has 2 `<h1>` elements ("Küpsiste poliitika" and "Privacy Policy") and repeated vague link text including "here" ×2; W3C also warns the English body text is tagged `lang="et"` .
- **Solution:**
  - Keep a single `<h1>` ; demote the second to `<h2>` or scope it to the English section.
  - Replace "here" links with descriptive text or add `aria-label` .
  - Mark English passages with `lang="en"` on the wrapping element.

3J. Add a nonce-based CSP (low urgency for this site shape) `Security`

- **Impact:** XSS defense-in-depth
- **Problem:** Content-Security-Policy is missing, but the site signals show no auth, payments, user content or e-commerce on this page, so XSS impact is limited.
- **Solution:** When you add a login or user-generated content, 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'
```

3K. Harden WordPress surface and add SRI `Security`

- **Impact:** Supply-chain integrity, takeover paths
- **Problem:** Security basics flags the jsdelivr script without an `integrity` attribute, a reachable `/wp-admin/install.php`, and a login form on the default `/wp-login.php` path.
- **Solution:**
  - Add SRI to the iframemanager script:

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

  - Block the installer in `.htaccess`: `<Files "install.php">Require all denied</Files>`
  - Move or protect `/wp-login.php` (custom path or IP allowlist) and add rate limiting.

3L. Add Referrer-Policy, Permissions-Policy and COOP/CORP `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, and the `server: Apache / ZoneOS` header discloses stack details.
- **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 unset Server
```

3M. Add Referrer-Policy, Permissions-Policy, COOP/CORP and hide the server banner `Security`

- **Impact:** Information leakage, cross-origin isolation

- **Problem:** Referrer-Policy, Permissions-Policy, Cross-Origin-Opener-Policy and Cross-Origin-Resource-Policy are all missing, and the `Server: Apache / ZoneOS` header discloses the stack.
- **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
```

3N. Harden the WordPress surface (SRI, installer, login path) `Security`

- **Impact:** Supply-chain and takeover risk
- **Problem:** 1 of 1 cross-origin scripts lacks an `integrity` attribute, `/wp-admin/install.php` is reachable, and the login form is served on the default `/wp-login.php` path.
- **Solution:**
  - Add SRI to the jsDelivr iframemanager script (or self-host it):

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

  - Block the installer in `.htaccess`:

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

  - Move or protect the login path (custom login slug, HTTP auth on `/wp-login.php`, or a login rate-limit plugin).

3O. Disambiguate repeated link text `Accessibility`

- **Impact:** WCAG 2.4.4 link purpose
- **Problem:** The page repeats vague anchor text — "kontakt" ×3, "meist" ×2, "tooted" ×2, "ressursid" ×2, "liitu meiega" ×2 — which is ambiguous when links are read out of context.
- **Solution:**

- Extend the visible text ("Kontakt — logistikaosakond") or add `aria-label`:

```
<a href="/en/contact/" aria-label="Kontakt – inglise
keeles">kontakt</a>
```

  - Keep the visible label as a prefix of the accessible name so voice-control users can still target it.

3P. Give the JSON-LD block a concrete schema type `SEO`

- **Impact:** Rich results eligibility
- **Problem:** The single JSON-LD block parses as valid but its type resolves to "Unknown", and PSI's `structuredData` audit fails.
- **Solution:**
  - Emit an explicit `@type` — `Organization` plus `ContactPage` for this URL:

```
{"@context":"https://schema.org","@type":"ContactPage","name":"Kont
akt - estply","mainEntity":
{"@type":"Organization","name":"Estply","url":"https://estply.com/"
,"contactPoint":
{"@type":"ContactPoint","contactType":"sales","email":"info@estply.
com"}}}
```

  - Validate with Google's Rich Results Test after the change.