Audit Report: Avaleht - estply

Website: https://estply.com/
Date: 28.10.2026
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/kupsiste-poliitika
- https://estply.com/kupsiste-poliitika
- https://estply.com/kontakt

Summary of results

Overall Score: 71 / 100
Status: Needs Improvement

Site overall 71 is the mean of 5 pages. Scores range 63 (https://estply.com/en/2026/07/06/vineeri-kvaliteediklassid-selgeks) → 76 (https://estply.com/kontakt). Weakest page: Mobile PSI is 72 against desktop 92 — a 20-point gap driven almost entirely by CLS 0.491 on mobile (desktop 0.143), with the footer element accounting for a 0.481 shift; LCP 2.7 s and Speed Index 4.61 s add further drag. Accessibility is structurally weak despite a clean axe run (1 moderate violation): the page has zero headings of any level (h1–h6 all 0), and PSI flags `button-name` (weight 10) and `target-size` (weight 7) as outright failures. Security basics returned FAILED — HSTS, X-Frame-Options and X-Content-Type-Options are all missing, which caps the score below 90; with no auth, payments, UGC or commerce signals, CSP is a P3 rather than a P1. W3C reports 7 errors (5 from WP Rocket's `text/rocketlazyloadscript` + `defer` combination, 2 from srcset candidates missing width descriptors), and the document ships with `cache-control: max-age=0` despite WP Rocket being present. Confidence is medium because CrUX field values are all 0 ms p75 (no usable field data) and the LCP element could not be identified, so the hero-lazy-load finding is heuristic.

Per-page scores

 Needs Improvement · https://estply.com/

Score	Performance	Accessibility	Best Practices	SEO	Security
70	82	91	81	92	FAILED

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

Score	Performance	Accessibility	Best Practices	SEO	Security
63	72	91	100	100	FAILED

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

Score	Performance	Accessibility	Best Practices	SEO	Security
73	87	91	100	85	FAILED

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

Score	Performance	Accessibility	Best Practices	SEO	Security
73	88	91	100	92	FAILED

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

Score	Performance	Accessibility	Best Practices	SEO	Security
76	87	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/	**82** / 96	**4.65 s** / 1.14 s	0.000 / **0.003**
https://estply.com/en/2026/07/06/vineeri-kvaliteediklassid-selgeks	**72** / 92	**2.72 s** / 866 ms	**0.491** / 0.143

URL	Performance (M / D)	LCP (M / D)	CLS (M / D)
https://estply.com/en/kupsiste-poliitika	**87** / 99	**3.87 s** / 818 ms	0.000 / 0.000
https://estply.com/kupsiste-poliitika	**88** / 99	**3.77 s** / 843 ms	0.000 / 0.000
https://estply.com/kontakt	**87** / 99	**3.85 s** / 966 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. Right-size the mobile hero image and repair srcset/sizes `Performance`

- **Impact:** LCP (4.7 s mobile), Speed Index, page weight
- **Problem:** The browser downloads a 1.94 MB 3200×1800 WebP for a 360×640 hero slot; images total 2.70 MB of the 2.76 MB page and PSI estimates 276 KiB of image-delivery savings. W3C confirms the markup is broken: `sizes="auto"` on an eager image and srcset candidates with no width descriptor.
- **Solution:**
  - Give the hero a correct `sizes` and a mobile-first candidate list so a ~360–720 px file is chosen:

```
<img src="/img/hero-720.webp"
     srcset="/img/hero-360.webp 360w, /img/hero-720.webp 720w,
/img/hero-1440.webp 1440w"
     sizes="(max-width: 720px) 100vw, 720px"
     width="360" height="640"
     fetchpriority="high" loading="eager" decoding="async"
     alt="ESTPLY birch plywood production">
```

  - Never emit `sizes="auto"` on a non-lazy image; every srcset candidate needs a width descriptor.
  - Re-encode the 3200×1800 source at ~80 quality — 1.94 MB is far above what a hero needs.
  - The hero currently has `alt=""`; give it descriptive alt text if it conveys content.

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, so the page can be framed and downgrade-stripped.
- **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"
Header always set Referrer-Policy "strict-origin-when-cross-origin"
```

Then submit the domain at hstspreload.org once the max-age is confirmed.

1C. Name the buttons and enlarge touch targets `Accessibility`

- **Impact:** WCAG 4.1.2 (name/role/value), 2.5.8 (target size), PSI accessibility score
- **Problem:** PSI's accessibility score of 91 is dragged down by two zero-scored audits: `button-name` (weight 10) — buttons have no accessible name — and `target-size` (weight 7) — touch targets lack sufficient size/spacing. axe-core's 0 violations do not cover these.
- **Solution:**
  - Add an accessible name to every icon-only button:

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

  - Ensure interactive targets are at least 44×44 px with ≥8 px spacing:

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

  - Also resolve the 17 color-contrast nodes axe marked incomplete (gradients/alpha) manually.

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

- **Impact:** CLS, mobile Performance score
- **Problem:** Mobile CLS is 0.491 (desktop 0.143) with a single footer element responsible for a 0.481 shift — well past the 0.25 heavy-penalty threshold.
- **Solution:**
  - Reserve space for the footer's late-injected content (cookie banner, iframe manager, or lazily-rendered blocks) with explicit `min-height` on `footer.footer`.
  - If the shift comes from a lazily loaded embed or font swap inside the footer, load it eagerly or set `font-display: optional` for the affected face.
  - Re-measure with Lighthouse mobile after each change; target CLS ≤ 0.1.

1E. Add HSTS, X-Content-Type-Options and X-Frame-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 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"
  ```

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

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

- **Impact:** LCP
- **Problem:** The optimized-web checklist fails 'Hero image eagerly loaded': the first raster image (`6c041c12…png`) has `loading="lazy"` and no `fetchpriority`, delaying LCP to 2.7 s on mobile.
- **Solution:**

  ```
  <img src="…/6c041c12fb0c531933532c08c2749a1a836d595a.png"
       alt="…" width="251" height="134"
       loading="eager" fetchpriority="high" decoding="async">
  ```

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

1G. Add a proper heading structure (currently zero headings) `Accessibility`

- **Impact:** WCAG 1.3.1 / 2.4.6, screen-reader navigation, SEO outline
- **Problem:** The heading outline 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 a single `<h1>`.
  - Mark section titles as `<h2>` and sub-sections as `<h3>`, in document order.
  - Do not skip levels; do not use styled `<div>`s in place of headings.

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

- **Impact:** LCP, FCP, Speed Index
- **Problem:** The Optimized-Web checklist fails 'Hero image eagerly loaded': the hero PNG (uploads/2026/08/6c041c12…png) has loading="lazy" and no fetchpriority, and mobile LCP is 3.9 s versus 0.8 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">
```

  - In WP Rocket, exclude the hero from LazyLoad (Media → LazyLoad → Excluded images) or add it to the 'Exclude from LCP/above-the-fold images' list.
  - Add `<link rel="preload" as="image" fetchpriority="high" href="…hero.png">` in `<head>`.

1I. Shorten the document latency and render-blocking chain `Performance`

- **Impact:** LCP, FCP, TTFB, Speed Index
- **Problem:** PSI flags document-latency-insight (est. 860 ms savings) and render-blocking-insight (est. 590 ms savings); the browser capture shows the document request taking 1.60 s and mobile FCP at 1.82 s.
- **Solution:**
  - Preload the critical font/CSS and preconnect to the only third-party origin:

```
<link rel="preconnect" href="https://cdn.jsdelivr.net" crossorigin>
```

  - Inline critical above-the-fold CSS and load the two external stylesheets non-blocking (`media="print" onload="this.media='all'"`).
  - Verify WP Rocket 'Remove Unused CSS' / 'Optimize CSS delivery' is enabled and that the HTML cache is warmed for this URL.
  - Investigate the 1.6 s document response: check for cold-cache misses and any server-side plugin work on the privacy-policy template.

1J. 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 is 91 with `button-name` scoring 0.00 (weight 10) and `target-size` scoring 0.00 (weight 7); axe found 0 violations but could not determine contrast on 7 nodes.
- **Solution:**
  - Add an accessible name to every icon-only button:

```
<button type="button" aria-label="Close cookie banner">
  <svg aria-hidden="true" focusable="false">…</svg>
```

```
</button>
```

- Ensure interactive targets are at least 44×44 px with adequate spacing (WCAG 2.5.8).
- Manually verify the 7 undetermined color-contrast nodes (gradients/alpha) with DevTools contrast checker.

1K. Stop returning 429 to legitimate traffic and put a page cache/CDN in front of the site `Performance`

- **Impact:** Availability, TTFB, LCP, audit coverage
- **Problem:** The audited URL responded `429 Too Many Requests` with a 337-byte body and `retry-after: 10`, so axe-core, the HTML inventory and the browser runtime captured an error page instead of the cookie policy; the optimized-web checklist also found no WordPress cache plugin or CDN edge cache marker.
- **Solution:**
  - Raise or remove the rate limit for normal browsing traffic and for monitoring/audit user agents; a single page view should never trip it.
  - Front the site with a page cache or CDN edge cache so repeat requests are served without hitting PHP.
  - Return a real HTML error page (with `lang`, viewport, title) for 429/5xx so crawlers and auditors see meaningful markup.
  - Verify with: `curl -sI https://estply.com/kupsiste-poliitika/ | head -20` — expect `200` and a `cache-control` / `x-cache` header.

1L. Add the three failed baseline security headers (HSTS, clickjacking protection, nosniff) `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 reported missing on the response.
- **Solution:** Send these from the origin (Apache shown; the response already discloses `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"
```

  - Prefer `Content-Security-Policy: frame-ancestors 'self'` once CSP is deployed; keep X-Frame-Options as the fallback for older browsers.

- Verify preload-list eligibility at hstspreload.org after the header is live.

1M. Make the LCP image eager and discoverable `Performance`

- **Impact:** LCP, FCP, Speed Index
- **Problem:** Mobile LCP is 3.9 s vs 1.0 s on desktop, and the optimized-web checklist fails "Hero image eagerly loaded": the hero (cz5i9178-100x100.webp) has `loading="lazy"` and no `fetchpriority`. PSI additionally flags `lcp-discovery-insight` and `document-latency-insight` (est. 1,170 ms savings) as high priority.
- **Solution:**
  - Remove `loading="lazy"` from the hero and add `fetchpriority="high"`:

```
<img src="/wp-content/uploads/2026/10/hero.webp"
     srcset="… 800w, … 1600w" sizes="100vw"
     width="1600" height="900"
     fetchpriority="high" decoding="async" alt="…">
```

  - Preload it in `<head>`: `<link rel="preload" as="image" href="…hero.webp" imagesrcset="…" imagesizes="100vw" fetchpriority="high">`
  - Keep `loading="lazy"` on everything below the fold (already correct for the other 21 images).
  - Investigate the 1,170 ms document-latency saving — check whether WP Rocket's page cache is warm for `/kontakt/` and whether the HTML can be served from CDN edge.

1N. Give icon 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 — the Lighthouse failures are real and the two tools disagree.
- **Solution:**
  - Add an accessible name to every button that only contains an icon or SVG:

```
<button type="button" aria-label="Sulge"><svg aria-hidden="true"
focusable="false">…</svg></button>
```

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

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

- Re-run Lighthouse mobile after the change to confirm both audits move off 0.00.

Priority 2: Important

Essential for compliance, user reach, and search visibility.

2A. Add a meta description `SEO`

- **Impact:** Search snippet CTR, PSI SEO score
- **Problem:** The document has no meta description — PSI's `meta-description` audit scores 0 and the HTML inventory confirms `Description: not set`.
- **Solution:** Add a 140–160 character description in the site's language (et), e.g.:

```
<meta name="description" content="ESTPLY toodab kvaliteetset kasevineeri Jõgevamaal – Baltikumi uusim vineeritehas, Lemeks Grupi tütarettevõte.">
```

  Also add a matching `og:description`.

2B. Break up the render-blocking dependency chain `Performance`

- **Impact:** FCP, LCP, Speed Index
- **Problem:** PSI's `render-blocking-insight` estimates 580 ms of savings and `network-dependency-tree-insight` scores 0, with Speed Index at 3.72 s on mobile.
- **Solution:**
  - Inline the critical above-the-fold CSS and defer the two external stylesheets.
  - Preload the hero image and the primary font:

```
<link rel="preload" as="image" href="/img/hero-720.webp" imagesrcset="/img/hero-360.webp 360w, /img/hero-720.webp 720w" imagesizes="(max-width: 720px) 100vw, 720px" fetchpriority="high">
<link rel="preload" as="font" type="font/woff2" href="/fonts/open-sans-regular.woff2" crossorigin>
```

  - Audit the 19 scripts — WP Rocket already defers 2; confirm the rest are not chained.

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

- **Impact:** XSS defense-in-depth

- **Problem:** CSP is missing entirely. The site is WordPress with a reachable admin login and the audit flagged a user-content signal (anchor href containing "upload"), so a script-injection foothold would be worth stealing.
- **Solution:** Use nonce + `'strict-dynamic'` 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, then enforce. `frame-ancestors 'self'` also closes the clickjacking gap.

2D. Harden the WordPress entry points `Security`

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

  - Put `/wp-login.php` behind rate limiting or a WAF rule, or front it with HTTP basic auth.
  - Add `Permissions-Policy: camera=(), microphone=(), geolocation=()` and `Cross-Origin-Opener-Policy: same-origin` while you are in the vhost.

2E. Fix the 11 W3C validation errors `Best Practices`

- **Impact:** Markup correctness, image selection, validator score
- **Problem:** W3C reports 11 errors: 5× `defer` on `type="text/rocketlazyloadscript"` data blocks, an empty `href` on a dns-prefetch link, `src` on a `<source>` element, `sizes="auto"` on an eager image, and two srcset candidates missing width descriptors.
- **Solution:**
  - Remove `defer` from the RocketLazyload data-block scripts (they are not executable JS).
  - Drop the empty `<link data-rocket-prefetch href="" rel="dns-prefetch">` or give it a real hostname.
  - Replace `<source src="data:image/svg+xml,…">` with a proper `<img>` fallback.

- Fix the srcset/sizes pairs flagged at lines 295, 306, 786 and 806 (see the hero-image fix above).

2F. Give buttons and icon controls accessible names `Accessibility`

- **Impact:** WCAG 4.1.2, PSI accessibility score
- **Problem:** PSI accessibility fails `button-name` (score 0.00, weight 10) — buttons on the page have no accessible name.
- **Solution:**
  - Add visible text or `aria-label` to every `<button>`:

```
<button type="button" aria-label="Open search">…</button>
```

  - For icon-only controls, pair the label with `aria-hidden="true"` on the SVG.

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

- **Impact:** WCAG 2.5.8, mobile usability
- **Problem:** PSI fails `target-size` (score 0.00, weight 7) — touch targets lack sufficient size or spacing on mobile.
- **Solution:**
  - Ensure every interactive element is at least 24×24 CSS px (WCAG 2.5.8 minimum) and ideally 44×44.
  - Add padding rather than enlarging the icon glyph:

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

2H. Stop sending cache-control: max-age=0 on the document `Performance`

- **Impact:** Repeat-visit TTFB, document latency
- **Problem:** The response sets `cache-control: max-age=0` even though WP Rocket is detected, and PSI's document-latency insight estimates 2,590 ms of savings; the browser runtime shows the document taking 2.46 s and 1.67 s.
- **Solution:**
  - In WP Rocket, enable page caching for this post type and confirm the `Cache-Control` header becomes something like `max-age=600, must-revalidate` for anonymous visitors.
  - Verify the cache is warmed for the canonical URL after deploy.
  - Ensure logged-in / dynamic regions bypass the cache rather than disabling it site-wide.

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

- **Impact:** W3C validation, responsive image selection
- **Problem:** W3C reports 2 errors: srcset values on the two `<img>` elements specify no width while a `sizes` attribute is present.
- **Solution:**

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

  Apply the same to the second image (`f2870486….png`).

2J. Remove defer from WP Rocket's data-block script tags `Best Practices`

- **Impact:** W3C validation (5 of 7 errors)
- **Problem:** W3C reports 5 errors: `<script type="text/rocketlazyloadscript" … defer>` — a data block must not carry `defer` .
- **Solution:**
  - In WP Rocket → File Optimization → Lazy Load, disable the 'delay JS execution' / rocketlazyloadscript rewriting for these tags, or exclude the affected scripts (cookieyes, etc.).
  - Alternatively, whitelist the script so it is emitted as a normal `<script type="text/javascript" defer>` .

2K. Add meaningful alt text to the two content images `Accessibility`

- **Impact:** WCAG 1.1.1, image SEO
- **Problem:** Both raster images on the page carry `alt=""` ; on an article about veneer quality classes these are almost certainly content images, not decoration.
- **Solution:**
  - Replace `alt=""` with a short description of what the image shows (e.g. the veneer grade being illustrated).
  - Keep `alt=""` only for genuinely decorative images.

2L. Add HSTS, X-Content-Type-Options and clickjacking protection `Security`

- **Impact:** Transport security, MIME sniffing, clickjacking
- **Problem:** Security basics FAILED: Strict-Transport-Security, X-Content-Type-Options and X-Frame-Options/frame-ancestors 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=31536000;
includeSubDomains; preload"
Header always set X-Content-Type-Options "nosniff"
Header always set Content-Security-Policy "frame-ancestors 'self'"
Header always set Referrer-Policy "strict-origin-when-cross-origin"
```

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

2M. Replace vague link text and collapse duplicate H1s `SEO`

- **Impact:** Link purpose (WCAG 2.4.4), document outline, SEO
- **Problem:** The inventory reports 2 `<h1>` elements ('Küpsiste poliitika' and 'Privacy Policy') plus repeated vague link text ('here' ×2, 'code of conduct' ×3, 'about us' ×2); PSI's `link-text` audit also fails with 2 links.
- **Solution:**
  - Keep exactly one `<h1>` per page; demote the second to `<h2>` or remove it.
  - Rewrite vague anchors to describe the destination:

```
<!-- before --><a href="/en/code-of-conduct">here</a>
<!-- after --> <a href="/en/code-of-conduct">Read the Estply code
of conduct</a>
```

  - Where the visible text must stay short, add `aria-label` with the full purpose.

2N. Stop sending max-age=0 on the HTML document `Performance`

- **Impact:** Repeat-visit TTFB, LCP
- **Problem:** The document response carries `cache-control: max-age=0` with an `expires` timestamp equal to the request time, forcing revalidation on every navigation despite WP Rocket being active.
- **Solution:**
  - Confirm WP Rocket page caching is actually serving this URL (the browser capture shows a 1.60 s document fetch, suggesting a cache miss).
  - Exclude logged-out policy pages from any 'no-cache' rule and let the CDN/page cache serve them with a positive `max-age` plus `s-maxage`.

2O. Cut mobile LCP from 3.8 s by removing render-blocking work `Performance`

- **Impact:** LCP, FCP, Speed Index
- **Problem:** Mobile LCP is 3.8 s (desktop 0.8 s) with `render-blocking-insight` estimating 580 ms of savings, `document-latency-insight` 590 ms, and `unused-css-rules` 32 KiB.
- **Solution:**

- Inline critical above-the-fold CSS and load the rest non-blocking:

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

- Add `defer` to non-critical theme/plugin scripts currently in `<head>`.
- Preload the LCP image and serve it as WebP/AVIF with `fetchpriority="high"`.
- Purge unused CSS (32 KiB reported) via your build step or an unused-CSS plugin.

2P. Give buttons and icon links accessible names and enlarge touch targets `Accessibility`

- **Impact:** WCAG 4.1.2 name/role/value, 2.5.8 target size
- **Problem:** PSI accessibility audits `button-name` (score 0.00, weight 10) and `target-size` (score 0.00, weight 7) both fail on mobile, and the SEO `tapTargets` audit fails too.
- **Solution:**
  - Add visible text or `aria-label` to every button, e.g. `<button aria-label="Close cookie banner">`.
  - Ensure interactive targets are at least 44×44 px with adequate spacing:

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

2Q. Set a correct lang attribute on every page, including error pages `Accessibility`

- **Impact:** WCAG 3.1.1 language of page
- **Problem:** axe-core reports a serious `html-has-lang` violation (the captured 429 page had no `lang`), while the W3C validator saw `lang="et"` on the real page but flagged that the document appears to be in English.
- **Solution:**
  - Ensure the template always emits `<html lang="et">` (the site is Estonian — `kupsiste-poliitika` = cookie policy) and that the error/429 template does too.
  - If any page is genuinely English, switch that page's `lang` to `en` rather than relying on the validator's heuristic.

2R. Add a meta description and structured data `SEO`

- **Impact:** SEO score (92), SERP snippet quality
- **Problem:** PSI SEO is 92 with `meta-description` scoring 0.00 and `structuredData` failing; the HTML inventory also shows 0 Open Graph and 0 Twitter tags on the captured document.
- **Solution:**

```
<meta name="description" content="Estply privaatsuspoliitika –
kuidas me töötleme ja kaitseme teie isikuandmeid.">
```

  - Add `Organization` / `WebSite` JSON-LD sitewide and `WebPage` on this page.
  - Add `og:title`, `og:description`, `og:image` for social sharing.

2S. Deploy a nonce-based CSP plus Referrer-Policy and Permissions-Policy `Security`

- **Impact:** XSS defense-in-depth, referrer leakage, feature abuse
- **Problem:** Content-Security-Policy, Referrer-Policy and Permissions-Policy are all missing. The inferred `hasUserContent` signal comes from the contact form's `<textarea>`, not persisted public content, so this is calibrated to Priority 2 rather than Priority 1.
- **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'
```

  - WP Rocket injects inline scripts (`text/rocketlazyloadscript`), so generate the nonce in PHP and whitelist it on those tags.
  - Add the cheap ones now:

```
Referrer-Policy: strict-origin-when-cross-origin
Permissions-Policy: geolocation=(), microphone=(), camera=()
```

2T. Fix document caching (Cache-Control: max-age=0) `Performance`

- **Impact:** Repeat-visit TTFB, LCP
- **Problem:** The HTML document is served with `cache-control: max-age=0` and an `expires` value equal to the request time, so every navigation revalidates the full 172.8 KB decoded document despite WP Rocket being active.
- **Solution:**

- Let WP Rocket serve a browser-cacheable document, e.g. `Cache-Control: public, max-age=600, stale-while-revalidate=60`.
- Keep `max-age=0` only for logged-in or form-submission responses.
- Confirm the CDN/ZoneOS edge is caching `/kontakt/` and that the cache is warmed after deploy.

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

- **Impact:** Markup correctness, parser robustness
- **Problem:** W3C reports 18 errors and 24 warnings, dominated by 12× `script type="text/rocketlazyloadscript"` carrying a `defer` attribute, plus an empty `href` on a dns-prefetch link, two `srcset` candidates with no width descriptor, and a `charset` meta placed after the first 1024 bytes.
- **Solution:**
  - The 12 rocketlazyloadscript errors are a WP Rocket pattern; either drop `defer` from those data-block scripts or move the lazy-load rewrite to a real `type="text/javascript"` tag emitted at runtime.
  - Remove the empty prefetch: `<link data-rocket-prefetch href="" rel="dns-prefetch">` → delete or give it a real origin.
  - Add width descriptors to the two offending `srcset` values (lines ~1617 and ~1637): `srcset="…png 300w, …png 600w"`.
  - Move `<meta charset="utf-8">` into the first 1024 bytes of `<head>`.

Priority 3: Best Practice

Recommended for long-term maintainability.

3A. Improve document caching and switch to Brotli `Performance`

- **Impact:** Repeat-visit TTFB, transfer size
- **Problem:** The HTML document is served with `cache-control: max-age=0` and compression is gzip (ratio 0.246) rather than Brotli.
- **Solution:**
  - Let WP Rocket serve a short but non-zero HTML TTL, e.g. `Cache-Control: public, max-age=600, s-maxage=86400`.
  - Enable Brotli at the CDN/edge (`brotli on;` in nginx, or the CDN's Brotli toggle) — typically 15–20% smaller than gzip on HTML/CSS.

3B. Disambiguate repeated vague link text `Accessibility`

- **Impact:** WCAG 2.4.4 (link purpose), screen-reader navigation

- **Problem:** The inventory finds repeated identical link text: "meist" ×2, "tooted" ×2, "kontakt" ×2, "liitu meiega" ×2, "käitumiskoodeks" ×3, "tehase külastaja meelespea" ×2.
- **Solution:** Add context via `aria-label` or visually hidden text:

```
<a href="/ettevottest">Meist<span class="sr-only"> — ESTPLY
ettevõtte tutvustus</span></a>
```

3C. Add Subresource Integrity and trim header disclosure `Security`

- **Impact:** Supply-chain risk, fingerprinting
- **Problem:** The single cross-origin script (`cdn.jsdelivr.net/gh/orestbida/iframemanager@1.3.0`) has no `integrity` attribute, and the response discloses `Server: Apache / ZoneOS`.
- **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 with `openssl dgst -sha384 -binary file.js | openssl base64 -A`.
  - Strip or genericise the `Server` header (`ServerTokens Prod`).

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

- **Impact:** XSS defense-in-depth
- **Problem:** Content-Security-Policy is missing. Site signals show no auth, payments, user content or commerce, so the exploitable XSS surface is minimal — hence P3 rather than P1.
- **Solution:** When a login or user content is added, deploy a nonce + `'strict-dynamic'` policy rather than a flat allowlist:

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

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

- **Impact:** Privacy leakage, origin isolation
- **Problem:** Referrer-Policy, Permissions-Policy, Cross-Origin-Opener-Policy and Cross-Origin-Resource-Policy are all missing from the response.

- **Solution:**

```
Header always set Referrer-Policy "strict-origin-when-cross-origin"
Header always set Permissions-Policy "camera=(), microphone=(),
geolocation=()"
Header always set Cross-Origin-Opener-Policy "same-origin"
Header always set Cross-Origin-Resource-Policy "same-origin"
```

3F. Add SRI to the jsdelivr script and hide the Server header `Security`

- **Impact:** Supply-chain integrity, technology disclosure
- **Problem:** 1 of 1 cross-origin scripts (cdn.jsdelivr.net iframemanager) lacks an `integrity` attribute, and the response discloses `Server: Apache / ZoneOS`.
- **Solution:**
  - Add `integrity="sha384-…" crossorigin="anonymous"` to the jsdelivr `<script>` tag, or self-host the file.
  - Suppress the version banner: `ServerTokens Prod` and `ServerSignature Off` in Apache.

3G. Harden WordPress entry points `Security`

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

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

  - Move the login form behind a custom path or add rate limiting / 2FA.

3H. Disambiguate repeated link text and validate structured data `SEO`

- **Impact:** Anchor-text relevance, rich results
- **Problem:** Repeated vague anchors ('code of conduct' ×3, 'about us' ×2, 'products' ×2, 'contact' ×2) and PSI's modeled SEO audit flags `structuredData`; the single JSON-LD block is typed 'Unknown'.
- **Solution:**
  - Give each repeated link a distinct accessible name via visible text or `aria-label`.

- Replace the untyped JSON-LD block with a valid `Article` / `BlogPosting` schema including `headline`, `datePublished`, `author` and `image`.

3I. Fix the 7 W3C validation errors `Best Practices`

- **Impact:** HTML validity, spec conformance
- **Problem:** W3C reports 7 errors and 2 warnings: 5× `script type="text/rocketlazyloadscript"` combined with `defer`, and 2× `srcset` candidates missing width descriptors while `sizes` is present.
- **Solution:**
  - WP Rocket's delayed-JS type is a data block, so `defer` is invalid on it — remove `defer` from those tags or let WP Rocket inject the script without the attribute.
  - Add width descriptors to the two `srcset` values:

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

3J. Close remaining WordPress hardening gaps `Security`

- **Impact:** Attack surface, information disclosure
- **Problem:** Security basics warns that `/wp-admin/install.php` is reachable, the login form is on the default `/wp-login.php` path, and the `server` header 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 + rate limiting / 2FA).
  - Strip or genericise the `Server` header (`ServerTokens Prod`, `Header unset X-Powered-By`).

3K. Manually verify the 7 undetermined contrast nodes `Accessibility`

- **Impact:** WCAG 1.4.3 Contrast
- **Problem:** axe-core returned 0 violations but flagged 7 nodes where it could not compute contrast (alpha transparency or gradients), so contrast compliance is unconfirmed.

- **Solution:**
  - Inspect each flagged node in DevTools and confirm ≥4.5:1 for body text and ≥3:1 for large text.
  - Re-run axe with the browser extension after any theme color changes to confirm the incomplete results clear.

3L. Add main/nav landmarks and a skip link `Accessibility`

- **Impact:** WCAG 1.3.1, 2.4.1 bypass blocks
- **Problem:** axe-core flags `landmark-one-main` and `region` (content in `h1`, `p`, `address` outside landmarks), and the HTML inventory found no `nav`, `main`, `header` or `footer` and no skip-to-content link.
- **Solution:**
  - Wrap the page in `<header>`, `<nav>`, `<main id="main">`, `<footer>`.
  - Add a skip link as the first focusable element:

```
<a class="skip-link" href="#main">Liigu põhisisu juurde</a>
```

  - Note: these were measured on the 429 error page — re-run the audit once the rate limit is lifted to confirm on the real template.

3M. Set an explicit Cache-Control policy on HTML responses `Performance`

- **Impact:** Repeat-visit TTFB, CDN hit rate
- **Problem:** The response carried no `cache-control`, `etag`, `last-modified` or `expires` header, which the header audit flags as a weak caching policy (measured on the 429 response, so re-verify on a 200).
- **Solution:**

```
# HTML: short cache with revalidation
Header set Cache-Control "public, max-age=600, stale-while-
revalidate=60"
# Static assets: long cache with hashed filenames
Header set Cache-Control "public, max-age=31536000, immutable"
```

3N. Manually verify the 109 unresolved color-contrast nodes `Accessibility`

- **Impact:** WCAG 1.4.3 Contrast (Minimum)
- **Problem:** axe-core returned 0 violations but marked 109 nodes as "incomplete" for color-contrast, meaning it could not compute the ratio (alpha, gradients or overlapping backgrounds) — this is unverified, not passing.
- **Solution:**

    - Run a contrast check in DevTools on the flagged nodes, especially text over images and gradient sections.
    - Target ≥4.5:1 for body text and ≥3:1 for large text (≥24 px or ≥18.66 px bold).
    - Where text sits on photos, add a solid overlay or scrim rather than relying on the image.

3O. Fix structured data and disambiguate repeated link text `SEO`

- **Impact:** Rich results eligibility, anchor-text quality
- **Problem:** PSI fails the `structuredData` audit and the single JSON-LD block is typed "Unknown"; the page also repeats vague anchors ("kontakt" ×3, "meist" ×2, "tooted" ×2, "info@estply.com" ×2).
- **Solution:**
    - Replace the untyped JSON-LD with a valid `Organization` + `ContactPage` graph including `name`, `url`, `telephone`, `address` and `contactPoint`.
    - Disambiguate repeated anchors with `aria-label` or surrounding context, e.g. `<a href="/meist" aria-label="Meist — Estply ettevõttest">meist</a>`.

3P. Add SRI to the jsDelivr script and trim remaining header gaps `Security`

- **Impact:** Supply-chain integrity, info disclosure
- **Problem:** 1 of 1 cross-origin scripts (iframemanager from cdn.jsdelivr.net) lacks an `integrity` attribute, the response discloses `Server: Apache / ZoneOS`, and COOP/CORP/X-Permitted-Cross-Domain-Policies are unset.
- **Solution:**
    - Pin and hash the third-party script:

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

    - Or self-host the 3 KB file to remove the third-party origin entirely.
    - Strip or genericise the `Server` header at the proxy.
    - Add `Cross-Origin-Opener-Policy: same-origin` and `X-Permitted-Cross-Domain-Policies: none`.

3Q. Close the remaining image-delivery and compression gaps `Performance`

- **Impact:** Page weight, transfer size

- **Problem:** Images account for 611.2 KB of the 682.9 KB page, PSI's `image-delivery-insight` still estimates 51 KiB of savings, and the document is served with gzip rather than brotli.
- **Solution:**
  - Audit the largest remaining images for over-sized dimensions (the srcset exposes 20 widths up to 2561 px — cap the top end at what the layout actually needs).
  - Enable brotli at the ZoneOS/CDN layer; gzip currently yields a 0.183 ratio on a 172.8 KB document.
  - Keep the existing WebP + srcset + explicit-dimension setup — it is already correct on 22/22 images.