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/tehase-kulastaja-meelespea
- https://estply.com/kaitumiskoodeks
- https://estply.com/tooalasest-rikkumisest-teavitamine
- https://estply.com/en

Summary of results

Overall Score: 70 / 100
Status: **Needs Improvement**

Site overall 70 is the mean of 5 pages. Scores range 66 (https://estply.com/tooalasest-rikkumisest-teavitamine) → 74 (https://estply.com/). Weakest page: Performance is the strongest area — PSI mobile 86 / desktop 100 with CLS 0.000 and TBT 0 ms — but mobile LCP of 3.9 s sits in the warning band and PSI flags 510 ms of document-latency savings plus a costly network dependency tree. Accessibility scores 92 mobile / 97 desktop, dragged down by two zero-scoring Lighthouse audits (`button-name` , `target-size`); the axe results (html-has-lang, landmark-one-main, region) were captured against a 429 error page and should not be read as real-site violations. The W3C validator did reach the real document and reports 26 errors, including 12 invalid `type="text/rocketlazyloadscript"` + `defer` scripts and 6 empty `aria-expanded` attributes. SEO is the weakest dimension: robots.txt returns HTTP 500, no meta description, no structured data, and tap targets fail. Security basics verdict is FAILED (HSTS, X-Frame-Options, X-Content-Type-Options all missing), which caps the overall below 90; the site also served a 429 to the auditor, so header and inventory data reflect that error response rather than the live page. Confidence is low because the runtime, HTML inventory and axe captures are all error-page artifacts that contradict the PSI render.

Per-page scores

 Needs Improvement · https://estply.com/

Score	Performance	Accessibility	Best Practices	SEO	Security
74	82	91	81	85	FAILED

 Needs Improvement · https://estply.com/tehase-kulastaja-meelespea

Score	Performance	Accessibility	Best Practices	SEO	Security
72	87	91	100	85	FAILED

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

Score	Performance	Accessibility	Best Practices	SEO	Security
70	84	91	100	85	FAILED

 Needs Improvement · https://estply.com/tooalasest-rikkumisest-teavitamine

Score	Performance	Accessibility	Best Practices	SEO	Security
66	86	92	100	85	FAILED

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

Score	Performance	Accessibility	Best Practices	SEO	Security
70	84	91	81	85	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** / 98	**4.80 s** / 602 ms	0.000 / **0.003**
https://estply.com/tehase-kulastaja-meelespea	**87** / 99	**3.78 s** / 845 ms	**0.010** / 0.000
https://estply.com/kaitumiskoodeks	**84** / 98	**4.34 s** / 1.03 s	0.000 / 0.000

URL	Performance (M / D)	LCP (M / D)	CLS (M / D)
https://estply.com/tooalasest-rikkumisest-teavitamine	**86** / 100	**3.93 s** / 803 ms	**0.000** / 0.000
https://estply.com/en	84 / **83**	**4.33 s** / 2.89 s	**0.009** / 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. Eliminate render-blocking resources and shorten the critical path `Performance`

- **Impact:** LCP, FCP, Speed Index
- **Problem:** PSI flags `render-blocking-insight` with an estimated 670 ms savings and `network-dependency-tree-insight` as a high-priority failure; mobile LCP is 4.8 s versus 0.6 s on desktop.
- **Solution:**
  - Inline critical above-the-fold CSS and defer the rest (`global.924fd86a1194f6c6.css` is 34.3 KB).
  - Preload the LCP image and its font with `<link rel="preload" as="image" fetchpriority="high">`.
  - Flatten the dependency chain: avoid CSS `@import` and chained stylesheet requests.
  - Keep WP Rocket's "Delay JS" / "Remove Unused CSS" enabled and verify the LCP element is not gated behind a deferred script.

1B. Cut image payload (2.70 MB of 2.76 MB total) `Performance`

- **Impact:** LCP, total page weight, mobile data cost
- **Problem:** Browser runtime shows 8 images totalling 2.70 MB out of a 2.76 MB page; PSI's `image-delivery-insight` estimates 276 KiB of savings.
- **Solution:**
  - Re-encode oversized JPEG/PNG sources to WebP/AVIF at the actual rendered dimensions (several images are 324×216 or 251×134 but likely served at full resolution).
  - Tighten the srcset ladder — 27 distinct widths is excessive; 4–5 breakpoints is enough.

- Add `decoding="async"` to below-the-fold images and confirm the hero (`kaasik-kaupo-kalda-360x640.webp`) is served at 2× DPR max.

1C. 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):

```
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. Fix robots.txt returning HTTP 500 `SEO`

- **Impact:** Crawlability, indexing
- **Problem:** PSI's `robots-txt` audit fails because the request for robots.txt returned HTTP status 500, and the SEO category sits at 85.
- **Solution:**
  - Serve a static `/robots.txt` with HTTP 200 rather than generating it dynamically through WordPress.
  - Minimum content:

```
User-agent: *
Allow: /
Sitemap: https://estply.com/sitemap_index.xml
```

  - Verify with Search Console's robots.txt tester after the fix.

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

- **Impact:** LCP, Speed Index
- **Problem:** Mobile LCP is 3.8 s vs 0.8 s on desktop, and the hero image (`…/2026/08/6c041c12….png`) is served with `loading="lazy"` and no `fetchpriority`; Lighthouse also flags `lcp-discovery-insight` and `document-latency-insight` (est. 2,060 ms savings).
- **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>` so it is discovered before the CSS/JS chain:

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

- Exclude the hero from WP Rocket's lazy-load ("Excluded images" setting) so the plugin does not re-add `loading="lazy"`.

1F. Add Strict-Transport-Security `Security`

- **Impact:** Transport security, downgrade/MITM protection
- **Problem:** The Security basics table marks Strict-Transport-Security as **fail** — the header is missing entirely, even though HTTP→HTTPS redirect works.
- **Solution:**

```
Header always set Strict-Transport-Security "max-age=31536000;
includeSubDomains; preload"
```

Only add `preload` once you are certain every subdomain is HTTPS-only, then submit at hstspreload.org.

1G. Eager-load and preload the LCP hero image `Performance`

- **Impact:** LCP, FCP, Speed Index
- **Problem:** Mobile LCP is 4.3 s versus 1.0 s on desktop, and the checklist flags the hero (estply-card-3-1-320x240.jpg) as loading="lazy" with no fetchpriority; PSI also fails lcp-discovery-insight.
- **Solution:**

- Remove `loading="lazy"` from the hero and add `fetchpriority="high"`:

```
<img src="/wp-content/uploads/2026/07/estply-card-3-1-320x240.jpg"
     srcset="... 320w, ... 480w, ... 960w, ... 1440w"
     sizes="(min-width: 960px) 960px, 100vw"
     width="960" height="720"
     fetchpriority="high" decoding="async" alt="…">
```

- Preload it in `<head>`: `<link rel="preload" as="image" href="…" imagesrcset="…" fetchpriority="high">`.
- Ensure the hero is not injected by JS (lcp-discovery-insight failure).

1H. Give every button and icon control an accessible name `Accessibility`

- **Impact:** WCAG 4.1.2, PSI accessibility score
- **Problem:** PSI's `button-name` audit scores 0.00 at weight 10 — buttons on the page have no accessible name.
- **Solution:**
  - Add visible text, `aria-label`, or a visually hidden span to each `<button>`:

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

  - Re-run axe/Lighthouse after the fix; `button-name` is a complete-failure audit, so any single unnamed button zeroes it.

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

- **Impact:** XSS mitigation, session/data protection
- **Problem:** CSP is missing entirely, and the page links to an upload surface (site signals: user-generated content = yes), so injected script could persist into stored content.
- **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 out in Report-Only first, then enforce.
  - Note the site loads `cdn.jsdelivr.net` (iframemanager.js) — add it via nonce or self-host it.

1J. 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 (or CSP frame-ancestors) and X-Content-Type-Options are all missing on the response.
- **Solution:** Send from the origin (Apache shown):

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

Prefer `Content-Security-Policy: frame-ancestors 'self'` once CSP is in place. Note: these are high-level hygiene checks on HTTP headers, TLS, cookies and a few well-known exposed paths — PASS means the basics are in place, it does **not** mean the site is secure.

1K. Stop returning 429 to legitimate clients and crawlers `Best Practices`

- **Impact:** Availability, crawl budget, audit/monitoring reliability
- **Problem:** The audited URL returned HTTP 429 with `retry-after: 10` and a 337-byte error body, and the browser runtime logged "Failed to load resource: the server responded with a status of 429".
- **Solution:**
  - Raise or scope the rate limit so normal page loads, search bots and uptime monitors are not throttled (allowlist verified Googlebot/Bingbot by reverse DNS, not by User-Agent).
  - Serve a real HTML error page with `Retry-After` and correct status semantics instead of a bare 337-byte body.
  - Check whether the ZoneOS/Apache WAF rule is triggering on the query-less canonical URL.

1L. Cut mobile LCP from 4.3 s by fixing image delivery and document latency `Performance`

- **Impact:** LCP, Speed Index, page weight
- **Problem:** Mobile LCP is 4.3 s (desktop 2.9 s); the runtime capture shows 8 images at 2.70 MB of a 2.76 MB page, and Lighthouse's image-delivery-insight estimates 276 KiB of savings plus 880 ms from document-latency-insight.
- **Solution:**
  - Convert the remaining JPG/PNG assets (only the hero is WebP today) to WebP/AVIF with `<picture>` fallbacks.
  - Right-size the hero: the LCP element is served at 360×640 — verify the intrinsic size matches the rendered box and add `fetchpriority="high"` + `<link rel="preload" as="image" imagesrcset=...>`.
  - Investigate the 880 ms document-latency saving: check WP Rocket page-cache hit rate and any uncached query strings on `/en/`.
  - Re-measure with throttled mobile after each change.

Priority 2: Important

Essential for compliance, user reach, and search visibility.

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

- **Impact:** WCAG 4.1.2 name/role/value, 2.5.8 target size
- **Problem:** PSI fails `button-name` (score 0, weight 10) and `target-size` (score 0, weight 7) on mobile, dragging accessibility to 91.
- **Solution:**
  - Add an accessible name to every `<button>`: visible text, or `aria-label="Open menu"` on the `header__toggle`.
  - Ensure interactive targets are at least 24×24 px with adequate spacing (44×44 px recommended).
  - Re-run axe after the change; the current axe pass did not surface these because it ran on desktop DOM.

2B. Add a meta description `SEO`

- **Impact:** Search snippet CTR, SEO score
- **Problem:** HTML inventory shows `Description: not set` and PSI fails the `meta-description` audit.
- **Solution:** Add a unique 140–160 character description in the `<head>`:

```
<meta name="description" content="ESTPLY toodab Jõgevamaal
kvaliteetset kasevineeri Lemeks Grupi tehasena — kaasaegne
tootmine, usaldusväärne tarne ja tuge Sinu ärile.">
```

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

- **Impact:** XSS defense-in-depth
- **Problem:** CSP is missing entirely (both `content-security-policy` and `csp-is-strict` fail). The site is WordPress with a reachable `/wp-admin/install.php`, so an XSS foothold would be valuable even without front-end user content.
- **Solution:** Use nonces plus `'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'
```

  - Roll out in report-only mode first and watch for violations from WP Rocket, CookieYes and jsDelivr.
  - Add `integrity` to the jsDelivr `iframemanager.js` script (currently 1 of 1 cross-origin scripts lacks SRI).

2D. Fix the 14 W3C markup errors `Best Practices`

- **Impact:** HTML validity, parser robustness

- **Problem:** W3C reports 14 errors and 1 warning before truncation at line 877, including five `text/rocketlazyloadscript` scripts carrying `defer`, an empty `href` on a `dns-prefetch` link, `src` on `<source>`, and srcset candidates missing width descriptors.
- **Solution:**
  - Remove `defer` / `async` from `type="text/rocketlazyloadscript"` scripts (WP Rocket's lazyload placeholder type is not a JS MIME type).
  - Delete the empty `<link data-rocket-prefetch href="" rel="dns-prefetch">` at line 34.
  - Replace `<source src="data:image/svg+xml,…">` with a proper `<img>` fallback or `srcset`.
  - Add width descriptors to every srcset candidate on the two 251×134 PNGs (lines 794, 814).
  - Remove the stray `<br />` at line 877.

2E. Enable browser caching on the HTML document `Performance`

- **Impact:** Repeat-visit TTFB, LCP
- **Problem:** The document response sends `cache-control: max-age=0` with an `expires` value equal to the request time, so every navigation revalidates the full 88 KB HTML despite WP Rocket being active.
- **Solution:**
  - Set a short but non-zero document TTL with stale-while-revalidate:

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

  - Keep static assets on long-lived immutable caching (`max-age=31536000, immutable`).

2F. Add X-Frame-Options and X-Content-Type-Options `Security`

- **Impact:** Clickjacking, MIME-sniffing
- **Problem:** Both headers are missing — the page can be framed (clickjacking) and browsers may MIME-sniff responses.
- **Solution:**

```
Header always set X-Frame-Options "SAMEORIGIN"
Header always set X-Content-Type-Options "nosniff"
```

  If you later add a CSP, prefer `frame-ancestors 'self'` and keep X-Frame-Options as a fallback for older browsers.

2G. Fix robots.txt returning HTTP 500 `SEO`

- **Impact:** Crawlability, indexing
- **Problem:** Lighthouse reports `robots-txt` failing: "Request for robots.txt returned HTTP status: 500" — crawlers may treat the site as disallowed.
- **Solution:**
  - Check the server error log for the `/robots.txt` request.
  - If WordPress serves it virtually, disable the conflicting rule and serve a static file:

```
User-agent: *
Allow: /
Sitemap: https://estply.com/sitemap_index.xml
```

  - Verify with `curl -I https://estply.com/robots.txt` returning 200 and `Content-Type: text/plain`.

2H. Give every button an accessible name `Accessibility`

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

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

  - Icon-only controls must never rely on the SVG alone for their name.

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

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

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

- Add spacing between adjacent links in the footer/nav so targets do not overlap.

2J. Fix the 23 W3C validation errors `Best Practices`

- **Impact:** Markup correctness, parser recovery
- **Problem:** The validator reports 23 errors, including 12× `<script type="text/rocketlazyloadscript">` with `defer`, duplicate `placeholder` / `aria-required` / `aria-invalid` attributes at line 412, a `charset` meta after the first 1024 bytes, and a stray `<br>` that triggers "Cannot recover after last error".
- **Solution:**
  - Move `<meta charset="utf-8">` to the very first element inside `<head>` (before any `<script>`).
  - Remove the duplicated attributes on the date input at line 412 — keep one `placeholder`, one `aria-required`, one `aria-invalid`.
  - Ask WP Rocket to output lazy-loaded scripts without `defer` / `async` on `type="text/rocketlazyloadscript"` data blocks, or exclude those snippets from delay.
  - Fix the stray `<br />` at line 1268 (likely an unclosed element in the footer content).

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

- **Impact:** Transport security, MIME sniffing, clickjacking
- **Problem:** Security basics FAILED: Strict-Transport-Security, X-Frame-Options and X-Content-Type-Options are all reported missing on the HTTPS response.
- **Solution:**

```
Header always set Strict-Transport-Security "max-age=31536000;
includeSubDomains; preload"
Header always set X-Content-Type-Options "nosniff"
Header always set X-Frame-Options "SAMEORIGIN"
```

  - `frame-ancestors 'self'` in the CSP above supersedes X-Frame-Options once CSP ships.
  - Verify preload status at hstspreload.org after the max-age is live.

2L. Add a meta description and fix robots.txt `SEO`

- **Impact:** SEO score (85), SERP snippet, crawlability

- **Problem:** PSI SEO is 85 with `meta-description` failing (Description: not set) and `robots-txt` failing because the request returned HTTP status 500.
- **Solution:**
  - Add a unique description per page:

```
<meta name="description" content="Estply käitumiskoodeks — meie
põhimõtted, vastutustundlik tegutsemine ja koostöö tarnijatega.">
```

  - Fix the robots.txt 500: check the server/PHP handler for `/robots.txt`, or serve a static file:

```
User-agent: *
Allow: /
Sitemap: https://estply.com/sitemap_index.xml
```

2M. Serve modern image formats and trim image payload `Performance`

- **Impact:** LCP, page weight, image-delivery-insight
- **Problem:** PSI's image-delivery-insight estimates 142 KiB of savings, and the page still ships PNG/JPG assets (e.g. the two 251×134 PNGs) while total image bytes are 220 KB of 278 KB captured.
- **Solution:**
  - Convert PNG/JPG to WebP or AVIF with a `<picture>` fallback.
  - Keep the existing 4-width srcset (320/480/960/1440) but add width descriptors to every candidate — W3C flags two srcset entries with no width.
  - Re-check the two 251×134 PNGs: they are small decorative images and may be better as inline SVG.

2N. 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 document despite WP Rocket being active.
- **Solution:**
  - Set a short but non-zero document TTL with revalidation:

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

  - In WP Rocket, enable "Cache lifespan" for HTML and confirm the browser-cache option is on.

- Keep `Vary: Accept-Encoding` (already present).

2O. Wrap all content in landmarks `Accessibility`

- **Impact:** WCAG 1.3.1, screen-reader navigation
- **Problem:** axe reports 1 moderate `region` violation — `b:nth-child(15..17)` sit outside any landmark, even though nav/main/header/footer exist.
- **Solution:**
  - Move the stray `<b>` elements inside `<main>` or a `<section>` / `<aside>` landmark.
  - Verify with the Accessibility pane that no text node is orphaned outside header/nav/main/footer.

2P. Cut mobile LCP from 3.9 s `Performance`

- **Impact:** LCP, FCP, Speed Index, mobile Performance score
- **Problem:** Mobile LCP is 3.9 s (desktop 0.8 s) and PSI flags `document-latency-insight` with 510 ms of estimated savings plus a failing `network-dependency-tree-insight`.
- **Solution:**
  - Reduce server document latency (510 ms est. savings): enable full-page cache / CDN edge cache — the checklist reports no cache plugin or CDN marker on the document response.
  - Flatten the critical request chain: preload the LCP image and the main stylesheet, and remove render-blocking dependencies from the head.
  - Serve the LCP image as WebP/AVIF with explicit `width` / `height` and `fetchpriority="high"`; PSI's `image-delivery-insight` estimates 16 KiB of savings.

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

- **Impact:** WCAG 4.1.2 (name/role/value), 2.5.8 (target size), Lighthouse Accessibility score
- **Problem:** Lighthouse accessibility is 92 mobile / 97 desktop, with `button-name` (weight 10, score 0) and `target-size` (weight 7, score 0) both failing.
- **Solution:**
  - Add visible text or `aria-label` to every icon-only button, e.g. `<button class="header__toggle" aria-label="Open menu" aria-expanded="false">`.
  - Ensure interactive targets are at least 24×24 CSS px (44×44 recommended) with adequate spacing.

- Note the 6 W3C errors for `aria-expanded=""` — the attribute must be `"true"` or `"false"`, never empty.

2R. Clear the 26 W3C validation errors `Best Practices`

- **Impact:** Markup correctness, script execution, assistive-tech parsing
- **Problem:** The validator reports 26 errors, led by 12× `script type="text/rocketlazyloadscript"` with `defer`, 6× empty `aria-expanded`, a `charset` meta after the first 1024 bytes, and two `srcset` candidates missing width descriptors.
- **Solution:**
  - Move `<meta charset="utf-8">` to the first element inside `<head>`.
  - Replace the lazy-load script hack with native `loading="lazy"` / `defer` on real JavaScript MIME types, or use `type="text/plain"` data blocks without `defer` / `async`.
  - Set `aria-expanded` to `"false"` initially on all six accordion buttons.
  - Add width descriptors to every `srcset` candidate when `sizes` is present: `srcset="img-480.png 480w, img-960.png 960w"`.
  - Remove `autocomplete` from hidden inputs and fix the stray `<br />` near line 1201.

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

- **Impact:** SERP snippet quality, rich results eligibility
- **Problem:** PSI reports `meta-description` and `structured-data` failing; the HTML inventory confirms no description, no Open Graph/Twitter tags and no JSON-LD.
- **Solution:**

```
<meta name="description" content="…140–160 char summary of the
page…">
<script type="application/ld+json">
{"@context":"https://schema.org","@type":"WebPage","name":"…","desc
ription":"…"}
</script>
```

  Pick a schema type that matches the content (Article, FAQPage, Organization).

2T. Set an explicit caching policy `Performance`

- **Impact:** Repeat-visit TTFB, CDN offload, document latency
- **Problem:** The response has no `cache-control`, `etag`, `last-modified` or `expires` header, and the checklist reports no page cache plugin or CDN edge

cache detected.

- **Solution:**

```
# HTML documents
Header set Cache-Control "public, max-age=600, s-maxage=3600,
stale-while-revalidate=60"
# Hashed static assets
Header set Cache-Control "public, max-age=31536000, immutable"
```

Pair with a page cache or CDN so the origin is not hit on every request.

2U. Add clickjacking and MIME-sniffing protection `Security`

- **Impact:** Clickjacking, MIME confusion
- **Problem:** Neither X-Frame-Options nor CSP `frame-ancestors` is set, and X-Content-Type-Options is missing — both are basic-tier failures in the Security basics table.
- **Solution:**

```
Header always set X-Frame-Options "SAMEORIGIN"
Header always set X-Content-Type-Options "nosniff"
```

Once a CSP is in place, `frame-ancestors 'self'` supersedes X-Frame-Options.

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

- **Impact:** Repeat-visit TTFB, back/forward cache
- **Problem:** The HTML response carries `cache-control: max-age=0` with an `expires` timestamp in the past, despite WP Rocket being detected — every repeat visit revalidates the document.
- **Solution:**
  - In WP Rocket, confirm page caching is actually active for `/en/` and that no cookie or query string is bypassing it.
  - Target a short but non-zero TTL for anonymous HTML:

```
Cache-Control: public, max-age=600, s-maxage=3600, stale-while-
revalidate=60
```

  - Keep `no-cache` only for logged-in or cart sessions.

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

- **Impact:** Markup correctness, responsive image selection

- **Problem:** The validator reports 17 errors before truncating at line 867, including IDs containing whitespace (`id="about the company"` , `id="guaranteed-quality- in-every-layer"`), srcset candidates without width descriptors, and `text/rocketlazyloadscript` data blocks carrying `defer` / `async` .
- **Solution:**
  - Replace spaces in IDs with hyphens: `id="about-the-company"` , `id="guaranteed-quality-in-every-layer"` .
  - Add width descriptors to every srcset candidate when `sizes` is present:

```
<img srcset="a-251x134.png 251w, a-502x268.png 502w" sizes="(max-
width:768px) 100vw, 251px" ...>
```

  - Remove `defer` / `async` from `type="text/rocketlazyloadscript"` blocks (WP Rocket rewrites these at runtime).
  - Remove the empty `href=""` on the dns-prefetch link and the stray `<br />` at line 867.

Priority 3: Best Practice

Recommended for long-term maintainability.

3A. Wrap all content in landmarks `Accessibility`

- **Impact:** WCAG 1.3.1 info and relationships
- **Problem:** axe reports one moderate `region` violation — three `<b>` elements (nth-child 15–17) sit outside any landmark, even though header/nav/main/footer are present.
- **Solution:** Move the stray `<b>` nodes inside `<main>` or the relevant `<section>` , or wrap them in a labelled `<aside aria-label="…">` .

3B. Add remaining hardening headers and block the installer `Security`

- **Impact:** Privacy, origin isolation, attack surface
- **Problem:** Referrer-Policy, Permissions-Policy, COOP and CORP are all missing; `/wp-admin/install.php` is reachable 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 unset Server
```

Block the installer in `.htaccess`:

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

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

- **Impact:** Rich results eligibility, anchor-text clarity
- **Problem:** The single JSON-LD block parses as type `Unknown`, and repeated vague anchors appear (`meist` ×2, `tooted` ×2, `kontakt` ×2, `liitu meiega` ×2).
- **Solution:**
  - Emit `Organization` and `WebSite` schema with `name`, `url`, `logo` and `sameAs`.
  - Disambiguate repeated anchors with `aria-label` or surrounding context, e.g. `<a href="/en/about/" aria-label="About ESTPLY">meist</a>`.

3D. Resolve the deprecated-API warning `Best Practices`

- **Impact:** Lighthouse Best Practices score (81)
- **Problem:** PSI's `deprecations` audit fails with 1 warning found, contributing to a Best Practices score of 81 on both mobile and desktop.
- **Solution:**
  - Open Chrome DevTools Issues panel and identify the flagged API.
  - Common culprits on WordPress are legacy `document.write`, synchronous XHR, or deprecated `unload` handlers in theme/plugin scripts such as `core.7c21cc2eb9f1534d.js`.

3E. Add a nonce-based CSP (when the site gains interactive surfaces) `Security`

- **Impact:** XSS defense-in-depth
- **Problem:** Content-Security-Policy is missing. Site signals show no auth, payments, user content or e-commerce, so XSS impact is currently low — hence P3 rather than P1.
- **Solution:** If you add a login, form submissions with stored data, or user 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'
```

3F. 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 reported missing.
- **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"
```

3G. Reduce technology disclosure and block the installer `Security`

- **Impact:** Attack surface
- **Problem:** The `Server: Apache / ZoneOS` header discloses the stack, and `/wp-admin/install.php` is reachable (harmless while installed, but an open takeover path if the database is ever unreachable). 1 of 1 cross-origin scripts also lacks an `integrity` attribute.
- **Solution:**
  - `Header unset Server` (or use `ServerTokens Prod`).
  - Block the installer:

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

  - 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. Fix srcset width descriptors `Best Practices`

- **Impact:** Responsive image selection, HTML validity
- **Problem:** Both `<img>` elements use `srcset` without width descriptors while `sizes` is present — the validator rejects the value.
- **Solution:**

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

3I. Disambiguate repeated link text and add structured data `SEO`

- **Impact:** Anchor-text relevance, rich results
- **Problem:** 8 link texts repeat verbatim (e.g. "meist" ×2, "tooted" ×2, "kontakt" ×2) and the single JSON-LD block has an unrecognised type, so Lighthouse fails `structuredData`.
- **Solution:**
  - Add `aria-label` or visually hidden context to repeated nav/footer links, e.g. `<a href="/meist" aria-label="Meist — ESTPLY ettevõttest">meist</a>`.
  - Replace the unknown JSON-LD type with a valid schema.org type (`Organization`, `WebPage`, or `BreadcrumbList`) and validate in the Rich Results Test.

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

- **Impact:** Repeat-visit TTFB, document latency
- **Problem:** The document response carries `cache-control: max-age=0` with an `expires` equal to the request time, so returning visitors re-download the 127 KB HTML even though WP Rocket is active.
- **Solution:**
  - In WP Rocket, enable browser caching for HTML and set a short but non-zero TTL (e.g. `max-age=600`).
  - Verify with `curl -I https://estply.com/tehase-kulastaja-meelespea/` that `cache-control` no longer reports `max-age=0`.

3K. Clean up the 10 W3C validation errors `Best Practices`

- **Impact:** HTML validity, script execution order
- **Problem:** W3C reports 10 errors: 5× `text/rocketlazyloadscript` with `defer`, 1× with `async`, 2× srcset entries missing width descriptors, and a stray `<br>` at line 580 that truncated the validator.
- **Solution:**
  - WP Rocket's lazyload rewrites `type` to `text/rocketlazyloadscript`; `defer` / `async` are invalid on a non-JS type. Exclude those tags from

lazyload in WP Rocket settings, or move them to a real `type="module"` /JS MIME type.
    - Add width descriptors to the two srcset values flagged at lines 497 and 517.
    - Remove the stray `<br />` before `<b>Fa…` at line 580.

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

- **Impact:** Privacy, origin isolation, third-party integrity
- **Problem:** Referrer-Policy, Permissions-Policy, Cross-Origin-Opener-Policy and Cross-Origin-Resource-Policy are all missing, the `Server: Apache / ZoneOS` header discloses the stack, and the single cross-origin script (cdn.jsdelivr.net) 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 X-Permitted-Cross-Domain-Policies "none"
ServerTokens Prod
ServerSignature Off
```

    - Add `integrity` + `crossorigin` to the jsDelivr script tag, or self-host iframemanager.js.

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

- **Impact:** Rich results, anchor-text relevance
- **Problem:** PSI's `structuredData` audit fails and the single JSON-LD block has type "Unknown"; 8 anchor texts repeat verbatim (e.g. "käitumiskoodeks" ×4, "kontakt" ×2).
- **Solution:**
    - Emit a valid `Organization` / `WebPage` / `BreadcrumbList` graph with `@context` and `@type`.
    - Disambiguate repeated links with `aria-label` or surrounding context, e.g. `<a href="/meist" aria-label="Meist — Estply tutvustus">meist</a>`.

3N. Block the reachable WordPress installer `Security`

- **Impact:** Attack surface
- **Problem:** Security basics reports `/wp-admin/install.php` is reachable — harmless while installed, but an open takeover path if the database ever becomes unreachable.

- **Solution:**

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

  - Or block `/wp-admin/install.php` at the edge/WAF.

3O. 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 e-commerce, so the exploitable XSS surface is minimal — hence P3 rather than P1.
- **Solution:** When you do add one, 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'
```

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

- **Impact:** Information leakage, feature abuse, process isolation
- **Problem:** Referrer-Policy, Permissions-Policy, Cross-Origin-Opener-Policy and Cross-Origin-Resource-Policy are all reported missing.
- **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"
```

  Also consider suppressing the `Server: Apache / ZoneOS` banner to reduce technology disclosure.

3Q. Eliminate the forced reflow in core.js `Performance`

- **Impact:** Main-thread work, INP
- **Problem:** Lighthouse's `forced-reflow-insight` scores 0.00, and `core.7c21cc2eb9f1534d.js` produces a 53 ms long task on mobile.
- **Solution:**
  - Batch DOM reads before writes in the theme's `core.js`; avoid `offsetHeight` / `getBoundingClientRect()` inside loops that also mutate

styles.

- Defer any layout measurement until after `requestAnimationFrame`.

3R. Add valid structured data `SEO`

- **Impact:** Rich results eligibility
- **Problem:** The `structured-data` audit fails and the single JSON-LD block is typed "Unknown", so no rich-result entity is recognized.
- **Solution:** Emit `Organization` + `WebSite` on the homepage and `Product` / `BreadcrumbList` where relevant:

```
{"@context":"https://schema.org","@type":"Organization","name":"EST
PLY","url":"https://estply.com/en/","logo":"https://estply.com/logo
.png"}
```

Validate with the Rich Results Test.

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

- **Impact:** Supply-chain integrity, referrer leakage, origin isolation
- **Problem:** 1 of 1 cross-origin scripts (jsDelivr iframemanager) lacks an `integrity` attribute; Referrer-Policy, Permissions-Policy, COOP and CORP are all missing; the `Server: Apache / ZoneOS` header discloses stack details.
- **Solution:**

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

```
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"
ServerSignature Off
```