Audit Report: Avaleht - estply

Website: https://estply.com/
Date: 31.10.2026
Audit Coverage: 100% — all sources returned data
Confidence: high

Pages Audited (5 of 5):

- https://estply.com/
- https://estply.com/en/privacy-policy/
- https://estply.com/privaatsuspoliitika/
- https://estply.com/kupsiste-poliitika/
- https://estply.com/kontakt/

Summary of results

Overall Score: 85 / 100
Status: Needs Improvement

Site overall 85 is the mean of 5 pages. Scores range 84 (https://estply.com/) → 87 (https://estply.com/kontakt/). Weakest page: Performance is excellent — PSI mobile 99 / desktop 94, LCP 1.1 s, CLS 0.000, TBT 0 ms mobile — and CrUX field data is 'fast' on every metric except mobile TTFB (1093 ms p75, 'average'). The main drags are elsewhere: 2.66 MB of images out of a 2.72 MB page (PSI image-delivery-insight estimates 231 KiB savings, and only the hero is WebP), two failing accessibility audits in PSI (button-name weight 10, target-size weight 7) despite axe reporting 0 violations, and a missing meta description that caps SEO at 92. Security basics PASS, but advanced header checks fail — the CSP is only `frame-ancestors 'self'` with no default-src or object-src, and Referrer-Policy, Permissions-Policy, COOP and CORP are all absent. W3C reports 11 errors (mostly WP Rocket lazyload script `type` / `defer` conflicts and malformed srcset/sizes), which is in the warning band. Desktop is slightly worse than mobile on TBT (169 ms vs 0 ms) and Speed Index, but the divergence is small and does not change the verdict.

Per-page scores

 Needs Improvement · https://estply.com/

Score	Performance	Accessibility	Best Practices	SEO	Security
84	99	91	100	92	PASS

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

Score	Performance	Accessibility	Best Practices	SEO	Security
84	99	91	100	85	PASS

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

Score	Performance	Accessibility	Best Practices	SEO	Security
84	100	91	100	92	PASS

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

Score	Performance	Accessibility	Best Practices	SEO	Security
84	98	91	100	92	PASS

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

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

PageSpeed Insights — Mobile vs Desktop

*Lower is worse for Performance; higher is worse for LCP and CLS. Worse value is **bolded**.*

URL	Performance (M / D)	LCP (M / D)	CLS (M / D)
https://estply.com/	99 / **94**	**1.05 s** / 301 ms	0.000 / 0.000
https://estply.com/en/privacy-policy/	**99** / 100	**1.05 s** / 281 ms	0.000 / 0.000
https://estply.com/privaatsuspoliitika/	100 / 100	**1.05 s** / 281 ms	0.000 / 0.000
https://estply.com/kupsiste-poliitika/	**98** / 99	**1.05 s** / 281 ms	0.000 / 0.000

URL	Performance (M / D)	LCP (M / D)	CLS (M / D)
https://estply.com/kontakt/	100 / 100	**1.05 s** / 281 ms	0.000 / 0.000

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. Give every button an accessible name `Accessibility`

- **Impact:** WCAG 4.1.2 Name, Role, Value; PSI accessibility score
- **Problem:** PSI's `button-name` audit scores 0.00 with weight 10 — buttons on the page have no accessible name, even though axe-core reported 0 violations (axe likely skipped icon-only controls).
- **Solution:** Add visible text or an `aria-label` to each button:

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

  If the button only wraps an icon, also add `aria-hidden="true"` to the SVG so the label is not doubled.

1B. Enlarge touch targets to 44×44 px `Accessibility`

- **Impact:** WCAG 2.5.8 Target Size; PSI `target-size` audit (weight 7)
- **Problem:** PSI's `target-size` audit scores 0.00 — touch targets lack sufficient size or spacing, which is a real problem on the mobile-first index.
- **Solution:**
  - Ensure every link/button is at least 24×24 CSS px (44×44 recommended) or has 24 px of spacing.
  - Common offenders: footer social icons, breadcrumb links, and small inline text links.

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

1C. Enlarge touch targets to 24×24 px minimum (44×44 recommended) `Accessibility`

- **Impact:** WCAG 2.5.8 Target Size; Lighthouse `target-size` (weight 7)
- **Problem:** Lighthouse `target-size` scores 0.00 on mobile — interactive elements are too small or too tightly spaced for touch.
- **Solution:**

- Add padding rather than growing the icon: `a.icon { padding: 10px; min-width: 44px; min-height: 44px; display: inline-flex; align-items: center; justify-content: center; }`
- Ensure ≥8 px spacing between adjacent targets.
- Re-run Lighthouse mobile to confirm `target-size` passes.

1D. Enlarge touch targets to at least 24×24 px (44×44 recommended) `Accessibility`

- **Impact:** WCAG 2.5.8 Target Size; mobile usability
- **Problem:** PSI `target-size` fails with score 0.00 and weight 7, and the SEO category also flags `tapTargets`.
- **Solution:**
  - Ensure interactive elements have a minimum 44×44 CSS px hit area (24×24 is the WCAG 2.5.8 floor).
  - Add padding rather than enlarging icons:

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

  - Add spacing between adjacent links/footer items so targets do not overlap.

Priority 2: Important

Essential for compliance, user reach, and search visibility.

2A. Convert remaining JPG/PNG images to WebP/AVIF `Performance`

- **Impact:** Page weight, LCP, image-delivery-insight
- **Problem:** Browser runtime shows 8 images totalling 2.66 MB of a 2.72 MB page; only the hero is WebP, and PSI's image-delivery-insight estimates 231 KiB of savings.
- **Solution:**
  - Re-encode the large JPEG/PNG assets (`dsc_5118-648x432.jpg` , `estply-cta-1-1560x420.jpg` , the two 251×134 PNGs) as WebP/AVIF.
  - Serve via `<picture>` with a fallback:

```
<picture>
  <source type="image/avif" srcset="img-800.avif 800w, img-
1600.avif 1600w" sizes="(max-width:800px) 100vw, 800px">
  <img src="img-800.jpg" srcset="img-800.jpg 800w, img-1600.jpg
1600w" sizes="(max-width:800px) 100vw, 800px" width="800"
height="533" alt="…" loading="lazy">
</picture>
```

- The 28 distinct srcset widths are excessive; trim to 4–5 breakpoints per image.

2B. Add a meta description `SEO`

- **Impact:** SEO score (currently 92), SERP snippet quality
- **Problem:** HTML inventory reports `Description: not set`, and PSI's `meta-description` audit scores 0.00.
- **Solution:** Add a unique 140–160 character description per page:

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

Also give the single JSON-LD block a concrete `@type` (currently reported as `Unknown`) — `Organization` or `LocalBusiness` fits a manufacturer.

2C. Harden the Content-Security-Policy `Security`

- **Impact:** XSS defense-in-depth; CSP strictness check
- **Problem:** CSP is present but only sets `frame-ancestors 'self'` — no `default-src`, no `object-src 'none'`, and no script/resource restrictions.
- **Solution:** Add a nonce-based policy rather than a flat allowlist:

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

Note: this is a brochure site with no auth, payments or real user-generated content (the `upload` signal is a nav link, not a UGC surface), so treat this as hardening rather than an active exposure.

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

- **Impact:** HTML validity, image loading correctness
- **Problem:** W3C reports 11 errors: 5× `script type="text/rocketlazyloadscript"` with `defer`, 1× empty `href` on a `dns-`

`prefetch` link, 1× `async` on the same data-block script, and 4× srcset/sizes mismatches (missing width descriptors, `sizes` starting with `auto` on a non-lazy image).

- **Solution:**
  - In WP Rocket, disable "Delay JS execution" for the affected snippets, or change the injected `type` to `text/javascript` so `defer` / `async` are valid.
  - Remove the empty `<link data-rocket-prefetch href="" rel="dns-prefetch">` at line 35.
  - Fix the two `srcset` values at lines 793/813 to include width descriptors, e.g. `srcset="…png 251w"`.
  - Add `loading="lazy"` to the `sizes="auto…"` image at line 309, or drop the `auto` prefix.

2E. Reduce document TTFB and stop serving HTML with max-age=0 `Performance`

- **Impact:** TTFB (CrUX mobile 1093 ms p75), repeat-visit performance
- **Problem:** CrUX mobile TTFB is 1093 ms p75 ('average'), and the document response carries `cache-control: max-age=0`, so every navigation revalidates the full 87 KB HTML.
- **Solution:**
  - Enable WP Rocket page caching for anonymous visitors and serve cached HTML from the edge/CDN.
  - Raise the document cache lifetime for anonymous traffic:

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

  - Investigate origin response time (Apache/ZoneOS) — the 2.65 s document request in the runtime capture is the outlier.

2F. Load the hero image eagerly with high fetch priority `Performance`

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

```
<img src="…/6c041c12….png" width="251" height="134"
     loading="eager" fetchpriority="high" alt="">
```

Keep `loading="lazy"` on everything below the fold.

2G. Fix srcset candidates missing width descriptors `Performance`

- **Impact:** Responsive image selection, W3C validity
- **Problem:** W3C reports 2 errors: both `<img>` elements use `sizes` but their `srcset` entries specify no width, so the browser cannot pick a candidate.
- **Solution:**

```
<img src="…/6c041c12….png"
     srcset="…/6c041c12-251x134.png 251w, …/6c041c12-502x268.png
502w"
     sizes="(max-width: 600px) 100vw, 251px"
     width="251" height="134" alt="" loading="lazy">
```

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

2H. Tighten the Content-Security-Policy `Security`

- **Impact:** XSS defense-in-depth
- **Problem:** CSP is present but only as `frame-ancestors 'self'` — no `default-src`, no `object-src 'none'`, so it restricts nothing about scripts or resources.
- **Solution:** Add the missing directives (nonce-based, not a flat allowlist):

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

Roll out in report-only mode first (`Content-Security-Policy-Report-Only`) to catch inline WP Rocket and jsdelivr dependencies.

2I. Serve the HTML document from cache `Performance`

- **Impact:** TTFB, Speed Index
- **Problem:** The document response carries `cache-control: max-age=0` while CrUX field TTFB is 1093 ms mobile (rated 'average') — every visit re-generates the page despite WP Rocket being active.
- **Solution:**
  - Confirm WP Rocket page caching is enabled for this URL and that the privacy-policy page isn't in the exclusion list.

- Serve cached HTML with a short TTL plus revalidation, e.g. `Cache-Control: public, max-age=600, s-maxage=3600`.
- Warm the cache after deploy so the first visitor doesn't pay the cold-start cost.

2J. Cut render-blocking CSS and unused rules `Performance`

- **Impact:** Speed Index (3.57 s mobile), FCP
- **Problem:** PSI flags `render-blocking-insight` (est. 760 ms savings) and `unused-css-rules` (est. 32 KiB) on mobile; Speed Index is 3.57 s versus 1.03 s desktop.
- **Solution:**
  - Inline the critical above-the-fold CSS and defer `global.3578d4f0….css` (34.3 KB) with `media="print" onload="this.media='all'"`.
  - Purge unused rules from the theme stylesheet — 32 KiB of the 34 KB file is reported unused.
  - Re-measure Speed Index on mobile after the change.

2K. Disambiguate vague and repeated link text `SEO`

- **Impact:** WCAG 2.4.4, Lighthouse `link-text`
- **Problem:** Lighthouse `link-text` scores 0.00 (2 links) and the inventory shows 'here' ×2 plus repeated 'about us', 'products', 'resources', 'contact' anchors.
- **Solution:**
  - Replace 'here' with the destination: `<a href="/en/contact/">contact our data protection officer</a>`.
  - Where the visible text must stay short, add `aria-label` with the full purpose.
  - Add `aria-label` to repeated nav links that appear in both header and footer.

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

- **Impact:** WCAG 2.5.8 target size; mobile usability
- **Problem:** Lighthouse `target-size` scores 0.00 (weight 7) — touch targets lack sufficient size or spacing, which hurts mobile users on the cookie banner and footer links.
- **Solution:**
  - Ensure interactive elements are at least 24×24 CSS px (WCAG 2.5.8 minimum) and ideally 44×44 px.
  - Add padding rather than increasing font size:

```
.footer a, .cookie-consent button { display:inline-flex; align-
```

```
items:center; min-height:44px; min-width:44px; padding:0 12px; }
```

- Verify spacing between adjacent targets so a 24 px circle centred on each does not overlap.

2M. Fix W3C validation errors in lazyload script tags and srcset `Best Practices`

- **Impact:** HTML validity; lazy-load reliability
- **Problem:** W3C reports 8 errors: 5× `defer` and 1× `async` on `<script type="text/rocketlazyloadscript">` data blocks, plus 2× `srcset` candidates missing width descriptors while `sizes` is present.
- **Solution:**
  - WP Rocket's `text/rocketlazyloadscript` is a data block, so `defer` / `async` are invalid there — WP Rocket already rewrites these at runtime. Exclude the affected scripts from the lazyload optimisation in WP Rocket settings ("Excluded JavaScript Files") or disable "Delay JavaScript execution" for the cookie-consent script.
  - Add width descriptors to the two `srcset` values (lines 544 and 564):

```
<img src="…6c041c12….png" srcset="…6c041c12….png 251w"
sizes="251px" width="251" height="134" loading="lazy" alt="">
```

2N. Eliminate render-blocking resources to cut Speed Index `Performance`

- **Impact:** Speed Index, FCP, LCP
- **Problem:** `render-blocking-insight` estimates 580 ms of savings and Speed Index is 4.28 s on mobile (1.46 s desktop) — the lowest-scoring performance audit at 0.76.
- **Solution:**
  - Inline the critical above-the-fold CSS (WP Rocket → File Optimization → Optimize CSS delivery).
  - Defer the two external stylesheets (`34.6 KB` total) until after first paint.
  - Preload the font files (3 requests currently report 0 B transferred but still gate text paint).
  - Re-measure Speed Index after each change; target < 3.4 s on mobile.

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

- **Impact:** TTFB, repeat-visit performance
- **Problem:** The document response is served with `cache-control: max-age=0` , and CrUX mobile TTFB p75 is 1093 ms ('average') versus 751 ms on desktop.

- **Solution:**
  - Let WP Rocket / the CDN serve a short but non-zero browser TTL for HTML, e.g. `cache-control: public, max-age=600, s-maxage=86400`.
  - Keep `Vary: Accept-Encoding` (already present).
  - Confirm the edge cache is warmed for the canonical URL after each deploy.

2P. Harden the WordPress install and login paths `Security`

- **Impact:** Attack surface, brute-force exposure
- **Problem:** Security basics warns that `/wp-admin/install.php` is reachable and the login form is served on the default `/wp-login.php` path.
- **Solution:**

```
# Block the installer once the site is installed
<Files "install.php">
  Require all denied
</Files>

# Restrict wp-login.php to known IPs, or front it with a custom
path
<Files "wp-login.php">
  Require ip 203.0.113.0/24
</Files>
```

  - Add rate limiting / 2FA on the login endpoint (a plugin such as Limit Login Attempts or Wordfence).

2Q. Add a meta description to the contact page `SEO`

- **Impact:** Search snippet quality; PSI SEO score
- **Problem:** HTML inventory shows `Description: not set` and PSI fails the `meta-description` audit (score 0.00), holding SEO at 92 on both strategies.
- **Solution:** Add a unique, ~150-character description in the page head (or via the SEO plugin's per-page settings):

```
<meta name="description" content="Võta Estplyga ühendust —
kontaktandmed, logistika ja laadimise info ning meie meeskond.
Vastame tööpäeviti.">
```

  Also add `og:description` to match the existing Open Graph block.

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

- **Impact:** XSS mitigation; header hygiene

- **Problem:** CSP is only `frame-ancestors 'self'` — the audit flags missing `default-src` and `object-src 'none'`, so no script or resource restrictions exist. The page also contains a contact form with a `<textarea>`, so submitted input is reflected/stored somewhere.
- **Solution:** Add a nonce-based policy rather than a flat allowlist:

```
Content-Security-Policy: default-src 'self'; object-src 'none';
base-uri 'none';
  script-src 'nonce-{RANDOM}' 'strict-dynamic' https:;
  style-src 'self' 'unsafe-inline'; img-src 'self' data: https:;
  frame-ancestors 'self'; form-action 'self'; upgrade-insecure-
requests
```

  - WordPress + WP Rocket + jsdelivr will need nonce injection or `'strict-dynamic'` propagation; test in report-only mode first.
  - Keep `frame-ancestors 'self'` (already present) alongside `X-Frame-Options: SAMEORIGIN`.

2S. Reduce field TTFB and stop the document being uncacheable `Performance`

- **Impact:** TTFB, LCP, FCP (field)
- **Problem:** CrUX mobile TTFB is 1093 ms p75 ('average') while lab TTFB is 3 ms, and the document response carries `cache-control: max-age=0` with no ETag — every visit revalidates against origin.
- **Solution:**
  - Confirm WP Rocket page cache is actually serving this URL (the HTML shows `cache-control: max-age=0`, which suggests a cache bypass or a miss).
  - Exclude the contact page from dynamic-cookie bypass rules if it renders statically.
  - Add an ETag or serve `Cache-Control: public, max-age=600, s-maxage=86400` for anonymous visitors.
  - Check origin server response time and consider full-page CDN caching in front of Apache.

2T. Fix the 19 W3C HTML validation errors `Best Practices`

- **Impact:** Markup correctness, parser robustness
- **Problem:** W3C reports 19 errors: 12× `script type="text/rocketlazyloadscript"` with `defer`, 1× `charset` meta after the first 1024 bytes, 1× empty `href` on a `dns-prefetch` link, 2× `srcset` candidates missing widths, 2× hidden inputs with `autocomplete`.
- **Solution:**

- Move `<meta charset="utf-8">` to the very first line of `<head>` (before any script).
- Remove the empty `href` on the `data-rocket-prefetch` link or drop the tag.
- Add width descriptors to the two `srcset` values flagged at lines 1625 and 1645, e.g. `srcset="…png 1x"` or use `w` descriptors with `sizes`.
- Remove `autocomplete` from hidden Gravity Forms inputs.
- The 12 `rocketlazyloadscript` + `defer` errors come from WP Rocket; update the plugin or exclude those specific scripts from delay.

Priority 3: Best Practice

Recommended for long-term maintainability.

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

- **Impact:** Privacy leakage, cross-origin isolation
- **Problem:** All four headers are missing per the security headers scan (advanced checks: Referrer-Policy fail, Permissions-Policy fail, COOP fail, CORP fail).
- **Solution:**

```
Referrer-Policy: strict-origin-when-cross-origin
Permissions-Policy: camera=(), microphone=(), geolocation=(),
interest-cohort=()
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
```

3B. Add SRI to the jsDelivr script and enable HSTS preload `Security`

- **Impact:** Supply-chain integrity, HSTS coverage
- **Problem:** 1 of 1 cross-origin scripts (`cdn.jsdelivr.net/.../iframemanager.js`) lacks an `integrity` attribute, and HSTS is set without `preload`.
- **Solution:**
  - Add `integrity="sha384-…" crossorigin="anonymous"` to the jsDelivr `<script>`, or self-host the file.
  - Append `preload` once you are confident every subdomain is HTTPS-only:

```
Strict-Transport-Security: max-age=31536000; includeSubDomains;
preload
```

  Then submit at hstspreload.org.

3C. Harden the WordPress install surface `Security`

- **Impact:** Brute-force and takeover risk

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

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

  - Move or protect the login path (custom login slug plugin, or IP allowlist on `/wp-login.php`), and add rate limiting / 2FA.
  - Strip the `Server: Apache / ZoneOS` header (`ServerTokens Prod`, `ServerSignature Off`).

3D. Manually verify the 9 indeterminate color-contrast nodes `Accessibility`

- **Impact:** WCAG 1.4.3 Contrast (Minimum)
- **Problem:** axe-core returned 0 violations but flagged 9 nodes as 'incomplete' for color contrast — these are elements with gradients, alpha transparency or background images that axe cannot evaluate automatically.
- **Solution:**
  - Inspect each flagged node in DevTools with the contrast checker, including hover/focus states.
  - Target ≥4.5:1 for body text and ≥3:1 for large text (≥24 px or ≥18.66 px bold).
  - Pay particular attention to text over the hero image and any CTA buttons.

3E. Disambiguate repeated link text `SEO`

- **Impact:** WCAG 2.4.4 Link Purpose; crawlability
- **Problem:** HTML inventory lists 8 link texts repeated 2–3 times each ("käitumiskoodeks" ×3, "meist" ×2, "tooted" ×2, "kontakt" ×2, etc.), which is ambiguous for screen readers and search engines.
- **Solution:**
  - Add `aria-label` where context is not obvious, e.g. `<a href="/et/tooted/" aria-label="Tooted – vineeritooted">Tooted</a>`.
  - Where the repeats are nav vs. footer duplicates, differentiate with the surrounding heading or a visually-hidden span.

3F. Add the remaining hardening headers `Security`

- **Impact:** Referrer leakage, feature abuse, cross-origin isolation

- **Problem:** Referrer-Policy, Permissions-Policy, Cross-Origin-Opener-Policy and Cross-Origin-Resource-Policy are all missing; HSTS lacks `preload`; the jsdelivr script has no `integrity` attribute.
- **Solution:**

  ```
  Referrer-Policy: strict-origin-when-cross-origin
  Permissions-Policy: camera=(), microphone=(), geolocation=()
  Cross-Origin-Opener-Policy: same-origin
  Cross-Origin-Resource-Policy: same-origin
  Strict-Transport-Security: max-age=31536000; includeSubDomains;
  preload
  ```

  Add SRI to the CDN script:

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

  Submit the domain to hstspreload.org only after confirming every subdomain is HTTPS-only.

3G. Clean up WP Rocket lazyload script attributes `Best Practices`

- **Impact:** W3C validity (6 of 8 errors)
- **Problem:** W3C reports 5 errors for `type="text/rocketlazyloadscript"` carrying `defer` and 1 for the same type carrying `async` — a data-block script type must not have those attributes.
- **Solution:**
  - WP Rocket rewrites `src` to `data-rocket-src` and swaps `type` at runtime; the `defer` / `async` attributes should be dropped from the rewritten tag and re-applied by the loader.
  - If the plugin version can't be changed, exclude the affected scripts from lazyload in WP Rocket → File Optimization → Excluded JavaScript Files.
  - Re-validate at validator.w3.org after the change.

3H. Add structured data and verify contrast manually `SEO`

- **Impact:** Rich results eligibility, WCAG 1.4.3
- **Problem:** PSI `structuredData` fails and the single JSON-LD block is typed 'Unknown'; axe-core could not determine contrast on 7 nodes.
- **Solution:**

- Emit a valid `Organization` (or `WebPage`) JSON-LD block with `@context`, `@type`, `name`, `url`.
- Manually check the 7 undetermined contrast nodes with DevTools' contrast picker — axe skips elements with alpha transparency or gradients.
- Confirm the two `alt=""` images are genuinely decorative; if they convey meaning, give them alt text.

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

- **Impact:** XSS defense-in-depth
- **Problem:** CSP is only `frame-ancestors 'self'` — no `default-src`, no `object-src 'none'`, so it restricts nothing about scripts or resources. Site signals show no auth, payments, user content or commerce, so this is low-risk today.
- **Solution:** If you later add a login or accept user input, move to a nonce-based policy rather than a flat allowlist:

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

  Note the site loads `cdn.jsdelivr.net` (iframemanager) — a nonce + `'strict-dynamic'` approach avoids having to allowlist that host.

3J. Add HSTS preload and suppress the Server header `Security`

- **Impact:** Transport hardening; technology disclosure
- **Problem:** HSTS is `max-age=31536000; includeSubDomains` but lacks `preload`, and the response discloses `Server: Apache / ZoneOS`.
- **Solution:**
  - Append `preload` to HSTS and submit the domain at hstspreload.org:

```
Header always set Strict-Transport-Security "max-age=63072000;
includeSubDomains; preload"
```

  - Strip the server banner:

```
ServerSignature Off
Header unset Server
```

3K. Disambiguate repeated vague link text `SEO`

- **Impact:** Anchor-text quality; screen-reader link lists

- **Problem:** HTML inventory flags repeated vague anchors — "siin" ×2, "meist" ×2, "tooted" ×2, "kontakt" ×2 — which are ambiguous out of context.
- **Solution:**
  - Replace "siin" with descriptive text (e.g. "lugege privaatsuspoliitikat").
  - Where the visible text must stay short, add `aria-label`:

```
<a href="/kontakt/" aria-label="Võtke meiega ühendust">kontakt</a>
```

3L. Block the WordPress installer and move the login path `Security`

- **Impact:** Brute-force and takeover surface
- **Problem:** Security basics warns that `/wp-admin/install.php` is reachable and the login form is served on the default `/wp-login.php` path.
- **Solution:**

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

  - Add rate limiting / 2FA on `/wp-login.php`, or front it with a custom login slug via a security plugin.
  - Add `integrity` + `crossorigin` to the jsDelivr `iframemanager.js` script tag (1 of 1 cross-origin scripts lacks SRI).

3M. Tighten the Content-Security-Policy `Security`

- **Impact:** XSS defense-in-depth
- **Problem:** The CSP is only `frame-ancestors 'self'` — `default-src` is missing and `object-src` is not `'none'`. Site signals show no auth, payments, user content or e-commerce, so this is a P3 hardening item rather than an urgent one.
- **Solution:**
  - Add the cheap directives now:

```
Content-Security-Policy: frame-ancestors 'self'; object-src 'none';
base-uri 'self'; default-src 'self'
```

  - If a login or user content is ever added, move to a nonce + `'strict-dynamic'` policy rather than a flat allowlist.

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

- **Impact:** Privacy, cross-origin isolation, HSTS coverage
- **Problem:** Advanced checks fail for Referrer-Policy, Permissions-Policy, Cross-Origin-Opener-Policy and Cross-Origin-Resource-Policy; HSTS lacks the `preload` directive and the `Server: Apache / ZoneOS` header discloses the stack.
- **Solution:**

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

  - Submit the domain at hstspreload.org once the preload directive is live.

3O. Remove defer/async from WP Rocket's data-block scripts `Best Practices`

- **Impact:** W3C validity (8 errors)
- **Problem:** W3C reports 6 errors from `<script type="text/rocketlazyloadscript">` blocks carrying `defer` (×5) and `async` (×1) — attributes that are invalid on non-JavaScript data blocks.
- **Solution:**
  - These are emitted by WP Rocket's delay-JS execution feature. Either disable 'Delay JavaScript execution' for this template, or exclude the affected scripts (CookieYes, iframemanager) from delay.
  - Alternatively accept them as a known validator false-positive class and suppress the rule in CI.

3P. Add meaningful structured data `SEO`

- **Impact:** Rich results eligibility
- **Problem:** The single JSON-LD block is reported with type `Unknown`, and PSI's `structured-data` audit fails.
- **Solution:**
  - Emit a valid `WebPage` / `Organization` graph with `@context`, `@type`, `name`, `url` and `inLanguage` matching the `et` page.
  - Validate with the Rich Results Test after the change.

3Q. Verify the 6 unresolved color-contrast nodes `Accessibility`

- **Impact:** WCAG 1.4.3 Contrast (Minimum)

- **Problem:** axe-core returned 0 violations but flagged 6 nodes under 'Elements must meet minimum color contrast ratio thresholds' as incomplete — likely text over gradients or with alpha transparency.
- **Solution:**
  - Inspect each of the 6 nodes in DevTools and confirm text/background contrast is ≥ 4.5:1 (≥ 3:1 for large text).
  - Replace gradient or semi-transparent backgrounds behind body copy with a solid colour, or darken the text token.

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

- **Impact:** Image bytes (16 KiB estimated savings)
- **Problem:** `image-delivery-insight` estimates 16 KiB of savings and both raster images on the page are PNG with no WebP/AVIF variant.
- **Solution:**
  - Convert both uploads to WebP and reference them via `<picture>` with a PNG fallback.
  - Low absolute impact (30 KB of images total) — do this alongside the srcset fix rather than as a standalone project.

3S. Trim render-blocking CSS and unused CSS `Performance`

- **Impact:** FCP, LCP, Speed Index
- **Problem:** PSI flags `render-blocking-insight` with an estimated 580 ms of savings and `unused-css-rules` with 32 KiB unused, plus `image-delivery-insight` at 74 KiB.
- **Solution:**
  - Inline critical above-the-fold CSS and defer `global.3578d4f092e5450b.css` (34.3 KB) via `media="print" onload` or WP Rocket's Optimize CSS Delivery.
  - Purge unused selectors with PurgeCSS or the theme's build step.
  - Re-encode the largest remaining images to AVIF/WebP at the sizes actually rendered (74 KiB estimated savings).

3T. Add SRI to the jsDelivr script and suppress the Server header `Security`

- **Impact:** Supply-chain integrity, information disclosure
- **Problem:** 1 of 1 cross-origin scripts (`iframemanager.js` from cdn.jsdelivr.net) lacks an `integrity` attribute, and the response discloses `Server: Apache / ZoneOS` .
- **Solution:**

- Add `integrity` + `crossorigin="anonymous"` to the jsDelivr `<script>` tag (generate the hash from the exact pinned version).
- Suppress the banner: `ServerTokens Prod` and `ServerSignature Off` in Apache, or strip it at the CDN/proxy layer.

3U. Harden WordPress entry points `Security`

- **Impact:** Attack surface
- **Problem:** Security basics flags `/wp-admin/install.php` as reachable and the login form served on the default `/wp-login.php` path (both warnings).
- **Solution:**

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

  - Move the login form behind a custom path or a WAF rule, and rate-limit `/wp-login.php`.

3V. Verify the hero image is not lazy-loaded `Performance`

- **Impact:** LCP
- **Problem:** The optimized-web checklist fails 'Hero image eagerly loaded' — it detected `loading="lazy"` on the first image, but that image is a 100×100 thumbnail and lab LCP is already 1.1 s, so the heuristic likely mis-identified the LCP element.
- **Solution:**
  - Confirm the real LCP element in DevTools Performance panel.
  - If it is an `<img>`, set `loading="eager"` and `fetchpriority="high"` on it and keep `loading="lazy"` on everything below the fold.

3W. Manually verify contrast on the 6 undetermined nodes `Accessibility`

- **Impact:** WCAG 1.4.3 Contrast (Minimum)
- **Problem:** axe-core returned 0 violations but left 6 nodes 'incomplete' for color-contrast — typically text over gradients, images, or with alpha transparency.
- **Solution:**
  - Inspect the 6 flagged nodes in DevTools with the contrast checker.
  - Target ≥4.5:1 for body text and ≥3:1 for large text (≥24 px or ≥18.66 px bold).

3X. Fix the preload credentials-mode mismatch `Performance`

- **Impact:** Unused preload, wasted request

- **Problem:** Console warning: the preload for `…/theme/img/rings.svg` is not used because the request credentials mode does not match.
- **Solution:** Add `crossorigin` to the preload link so it matches the consuming request:

  ```
  <link rel="preload" href="/wp-content/themes/wordpress-base/inc/theme/img/rings.svg" as="image" type="image/svg+xml" crossorigin>
  ```

  Or remove the preload if the SVG is not on the critical path.