Audit Report: Vineeri kvaliteediklassid selgeks - estply

Website: https://estply.com/en/2026/07/06/vineeri-kvaliteediklassid-selgeks
Date: 29.10.2026
Audit Coverage: 100% — all sources returned data
Confidence: high

Pages Audited (1 of 1):

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

Summary of results

Overall Score: 68 / 100
Status: □ Needs Improvement

Mobile PSI is 70 (desktop 88), dragged down almost entirely by CLS 0.492 — the footer alone accounts for a 0.481 shift — and a Speed Index of 6.67 s, while TBT is 0 ms and LCP is a healthy 2.3 s. Accessibility scores 91/96 but the page has zero headings of any level (h1–h6 all 0), which axe flags as `page-has-heading-one` and which also hurts SEO outline; PSI additionally fails `button-name` and `target-size` at score 0. Security basics PASS, but the advanced tier shows a weak CSP (`frame-ancestors 'self'` only, no `default-src` / `object-src 'none'`), missing Referrer-Policy/Permissions-Policy/COOP/CORP, HSTS without preload, and no SRI on the jsdelivr script — with no auth, payments, UGC or commerce signals these are P3 hardening rather than P1. W3C reports 8 errors, mostly WP Rocket's `text/rocketlazyloadscript` blocks carrying `defer` / `async` plus two `srcset` candidates missing width descriptors. Image assets are in good shape (2 images, both with alt, dimensions and lazy loading), so the 15% image budget is not a drag; the CrUX field values returned as 0 ms p75 across LCP/TTFB/INP, which looks like an artifact rather than real field data.

Per-page scores

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

Score	Performance	Accessibility	Best Practices	SEO	Security
68	70	91	100	100	PASS

PageSpeed Insights — Mobile vs Desktop

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

Strategy	Performance (M / D)	LCP (M / D)	CLS (M / D)
Mobile vs Desktop	**70** / 88	**2.34 s** / 701 ms	**0.492** / 0.143

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.

Item	Status	Detail
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. Eliminate the 0.49 layout shift in the footer `Performance`

- **Impact:** CLS (0.492 mobile / 0.143 desktop), PSI Performance
- **Problem:** Lighthouse attributes a 0.481 shift to `div#page > div.main > div.main__footer > footer.footer`, pushing mobile CLS to 0.492 — well past the 0.25 heavy-penalty threshold.
- **Solution:**
  - Reserve space for anything injected into the footer (cookie banner, iframe-manager placeholder, lazy-loaded embeds) with a fixed `min-height` so it does not push content.
  - Give every footer image/iframe explicit `width` / `height` or `aspect-ratio`.
  - Avoid inserting DOM above the footer after first paint; render the consent banner in a fixed-position overlay instead of in-flow.
  - Re-run Lighthouse after each change and confirm the `cls-culprits-insight` footer entry disappears.

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

- **Impact:** Screen-reader navigation, SEO outline, axe `page-has-heading-one`
- **Problem:** HTML inventory reports h1 ×0, h2 ×0, h3 ×0, h4 ×0, h5 ×0, h6 ×0, and axe flags `page-has-heading-one` (moderate) on `html`.
- **Solution:**
  - Add exactly one `<h1>` containing the article title ("Vineeri kvaliteediklassid selgeks").
  - Break the body copy into `<h2>` / `<h3>` sections so the outline is meaningful.
  - Verify with the headings-map in DevTools that no level is skipped.

Priority 2: Important

Essential for compliance, user reach, and search visibility.

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

- **Impact:** LCP, Speed Index (6.67 s mobile)
- **Problem:** The optimized-web checklist fails "Hero image eagerly loaded": `…6c041c12fb0c531933532c08c2749a1a836d595a.png` has `loading="lazy"` and no `fetchpriority`, delaying the largest paint.
- **Solution:**

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

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

2B. Name all buttons and enlarge touch targets `Accessibility`

- **Impact:** PSI Accessibility (91 mobile), WCAG 4.1.2 / 2.5.8
- **Problem:** PSI fails `button-name` (score 0.00, weight 10) and `target-size` (score 0.00, weight 7) on mobile; axe's automated pass did not surface them, so they are likely icon-only controls.
- **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 (WCAG 2.5.8).
  - Re-test with keyboard-only navigation and a screen reader.

2C. Fix W3C validation errors from WP Rocket lazy-load and srcset `Best Practices`

- **Impact:** HTML validity (8 errors), image selection
- **Problem:** W3C reports 5 errors for `defer` and 1 for `async` on `type="text/rocketlazyloadscript"` data blocks, plus 2 `srcset` candidates missing width descriptors (lines 399, 419).
- **Solution:**
  - WP Rocket rewrites `<script>` to `type="text/rocketlazyloadscript"`; exclude the affected scripts (or the whole inline block) from "Delay JavaScript execution" so `defer` / `async` are not emitted on non-JS types.

- Add width descriptors to the two `srcset` values, e.g. `srcset="…png 251w"` with a matching `sizes` attribute.

Priority 3: Best Practice

Recommended for long-term maintainability.

3A. Harden the CSP beyond frame-ancestors `Security`

- **Impact:** XSS defense-in-depth
- **Problem:** CSP is only `frame-ancestors 'self'` — no `default-src`, no `object-src 'none'`, so no script or resource restrictions apply. Site signals show no auth, payments, UGC or commerce, so this is P3 rather than P1.
- **Solution:** If you later add login or user content, deploy a nonce-based policy rather than a flat allowlist:

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

  At minimum add `default-src 'self'` and `object-src 'none'` now — both are cheap and break nothing.

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

- **Impact:** Header hygiene, cross-origin isolation, third-party script integrity
- **Problem:** Referrer-Policy, Permissions-Policy, Cross-Origin-Opener-Policy and Cross-Origin-Resource-Policy are all missing; HSTS lacks `preload`; 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-site"
  Header always set Strict-Transport-Security "max-age=31536000;
  includeSubDomains; preload"
  ```

  Add `integrity` + `crossorigin="anonymous"` to the jsdelivr `iframemanager.js` tag, or self-host it.

3C. Stop serving the HTML document with cache-control max-age=0 `Performance`

- **Impact:** Repeat-visit TTFB, caching
- **Problem:** The document response returns `cache-control: max-age=0` with an `expires` timestamp in the past, so browsers revalidate the 66.9 KB HTML on every navigation despite WP Rocket being active.
- **Solution:**
  - In WP Rocket, enable browser caching for HTML and confirm the document is served with a positive `max-age` (e.g. `max-age=600, must-revalidate`).
  - Verify the header at the edge/CDN, not just at origin — a proxy may be overriding it.

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

- **Impact:** Link purpose (WCAG 2.4.4), rich results
- **Problem:** Repeated vague anchors ("code of conduct" ×3, "about us" ×2, "products" ×2, "contact" ×2) and PSI fails the `structuredData` audit; the single JSON-LD block is typed "Unknown".
- **Solution:**
  - Give each repeated link a distinct accessible name via `aria-label` or visually hidden text, e.g. `<a href="/en/about/">About us<span class="sr-only"> — Estply</span></a>`.
  - Replace the untyped JSON-LD with a valid `Article` / `BlogPosting` schema including `headline`, `datePublished`, `author` and `image`.

3E. Harden WordPress entry points `Security`

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

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

  - Move the login form behind a custom path or add rate limiting / 2FA.
  - Note: the Security basics PASS verdict covers headers, TLS and a few well-known paths only — it does not mean the site is secure.