Audit Report: Kawiare - Experience of Taste

Website: https://kawiare.ee/
Date: 2026-07-13

Overall Score: 56 / 100
Status: **Poor**
Confidence: high
Audit Coverage: 100% — all sources returned data

Pages Audited (10 of 10):

- https://kawiare.ee/
- https://kawiare.ee/artiklid
- https://kawiare.ee/kuidas-eristada-kvaliteetset-punast-kalamarja
- https://kawiare.ee/kaaviar-kui-looduslik-toidulisand-ehk-kaaviar-ilma-muutideta
- https://kawiare.ee/kuidas-ara-tunda-toeliselt-head-kaheksajalga
- https://kawiare.ee/kuidas-eristada-kvaliteetset-kaaviari
- https://kawiare.ee/kammkarp
- https://kawiare.ee/ahven-ja-koha
- https://kawiare.ee/lumekrabi
- https://kawiare.ee/kaaviar-tanapaeval

Summary

Site overall 56 is the mean of 10 pages. Scores range 45 (https://kawiare.ee/kuidas-eristada-kvaliteetset-punast-kalamarja) → 62 (https://kawiare.ee/kaaviar-tanapaeval). Weakest page: Mobile performance is critically low (63/100) with an LCP of 8.6 s, far exceeding the 2.5 s threshold and dragging the overall score. A critical security configuration error exists where HTTP traffic does not redirect to HTTPS, exposing users to downgrade attacks. Accessibility has a serious contrast violation and missing skip-link, though desktop performance is strong (95/100). Security headers are weak (40/100) with missing CSP and preload, but the HTTP redirect failure is the most urgent security fix. The site functions but requires significant optimization for mobile users and security hardening.

Per-Page Scores

Page	Score	Status	Confidence
https://kawiare.ee/	55	□ **Poor**	high
https://kawiare.ee/artiklid	48	□ **Poor**	high
https://kawiare.ee/kuidas-eristada-kvaliteetset-punast-kalamarja	45	□ **Poor**	high
https://kawiare.ee/kaaviar-kui-looduslik-toidulisand-ehk-kaaviar-ilma-muutideta	58	□ **Poor**	high
https://kawiare.ee/kuidas-ara-tunda-toeliselt-head-kaheksajalga	55	□ **Poor**	high
https://kawiare.ee/kuidas-eristada-kvaliteetset-kaaviari	62	□ **Needs Improvement**	high
https://kawiare.ee/kammkarp	62	□ **Needs Improvement**	high
https://kawiare.ee/ahven-ja-koha	55	□ **Poor**	high
https://kawiare.ee/lumekrabi	62	□ **Needs Improvement**	high
https://kawiare.ee/kaaviar-tanapaeval	62	□ **Needs Improvement**	high

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://kawiare.ee/	**49** / 71	**9.27 s** / 1.67 s	**1.000** / 0.637
https://kawiare.ee/artiklid	**61** / 89	**7.82 s** / 1.79 s	0.001 / **0.001**

URL	Performance (M / D)	LCP (M / D)	CLS (M / D)
https://kawiare.ee/kuidas-eristada-kvaliteetset-punast-kalamarja	**63** / 95	**8.65 s** / 1.51 s	0.000 / **0.000**
https://kawiare.ee/kaaviar-kui-looduslik-toidulisand-ehk-kaaviar-ilma-muutideta	**60** / 72	**8.49 s** / 1.77 s	0.000 / **0.000**
https://kawiare.ee/kuidas-ara-tunda-toeliselt-head-kaheksajalga	**60** / 91	**8.95 s** / 1.61 s	0.000 / **0.000**
https://kawiare.ee/kuidas-eristada-kvaliteetset-kaaviari	**60** / 94	**8.56 s** / 1.60 s	0.000 / **0.000**
https://kawiare.ee/kammkarp	**60** / 98	**8.48 s** / 1.01 s	0.000 / **0.000**
https://kawiare.ee/ahven-ja-koha	**68** / 94	**8.39 s** / 1.58 s	0.000 / **0.000**
https://kawiare.ee/lumekrabi	**65** / 94	**7.28 s** / 1.53 s	0.000 / **0.000**
https://kawiare.ee/kaaviar-tanapaeval	**56** / 95	**8.34 s** / 1.48 s	0.000 / **0.000**

Optimization Checklist

4 of 7 passing — 4 pass · 2 warn · 1 fail

Item	Status	Detail
Page caching plugin / CDN active	**Pass**	Caching plugin detected (WP Rocket)
Images lazy-loaded	**Pass**	All raster images use loading="lazy".
Hero image eagerly loaded	**Pass**	Hero image is eagerly loaded (inferred from DOM order/size — Lighthouse LCP element unavailable).
Hero is a real (not a CSS	**Warn**	Hero element uses a CSS background-image (no image-set() variants), so the browser always loads the original asset regardless of viewport — there is no srcset

Item	Status	Detail
background-image)		equivalent. Move the hero to a real with srcset/sizes (or) so smaller viewports can fetch a smaller file.
Responsive images (srcset /)	**Warn**	Only 15/22 raster images use srcset or (68%).
Reasonable number of image sizes	**Pass**	17 distinct srcset widths.
JS scripts not blocking in	**Fail**	5 render-blocking scripts in . Move to footer or add defer/async.

Fixes

Priority 1: Critical

Immediate action — impacts user experience, search rankings, or site safety.

1A. Optimize images for WebP and lazy loading

- **Impact:** LCP, Page Weight, CLS
- **Problem:** Images total 1.45 MB with no WebP format; 6 images missing loading='lazy' contribute to LCP 9.3 s.
- **Solution:** Convert all PNG/JPEG to WebP/AVIF. Add `loading="lazy"` to non-hero images. Ensure hero image has `fetchpriority="high"` .

```
<img src="image.webp" alt="..." loading="lazy" width="1200"
height="800">
```

1B. Defer non-critical JavaScript

- **Impact:** LCP, TBT, FCP
- **Problem:** 11 render-blocking scripts identified; main.js (163 KB) and GTM (64 KB) cause long tasks and delay rendering.
- **Solution:** Add `defer` or `async` to all non-critical scripts in `<head>`. Move WooCommerce/Contact Form scripts to footer if not needed for initial paint.

```
<script src="main.js" defer></script>
```

1C. Enforce HTTPS redirect for all HTTP traffic

- **Impact:** Security, Data Integrity

- **Problem:** Audit shows http://kawiare.ee/artiklid does not redirect to HTTPS, leaving users vulnerable to interception on unencrypted connections.
- **Solution:** Configure the web server (Apache/Nginx) to return a 301 redirect for all HTTP requests to the HTTPS equivalent:

```
RewriteEngine On
RewriteCond %{HTTPS} off
RewriteRule ^(.*)$ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]
```

1D. Defer or async non-critical JavaScript to fix LCP

- **Impact:** LCP, FCP, TBT
- **Problem:** 16 render-blocking scripts and 224 KB unused JS delay first paint; LCP is 7.8 s on mobile.
- **Solution:** Add `defer` or `async` to all non-critical scripts in `<head>`. For WordPress, use a plugin like 'WP Rocket' or 'Autoptimize' to defer JS, or manually update theme files:

```
<script src="main.js" defer></script>
```

1E. Force HTTPS Redirect

- **Impact:** Security, Transport Layer
- **Problem:** HTTP traffic (http://kawiare.ee/...) does not redirect to HTTPS, leaving users vulnerable to downgrade attacks and mixed content warnings.
- **Solution:** Configure the web server (Apache/Nginx) to redirect all HTTP requests to HTTPS:

```
RewriteEngine On
RewriteCond %{HTTPS} off
RewriteRule ^(.*)$ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]
```

1F. Optimize Largest Contentful Paint (LCP)

- **Impact:** Mobile Performance, LCP (8.6 s)
- **Problem:** Mobile LCP is 8.6 s (threshold 2.5 s), driven by render-blocking scripts and heavy resource loading.
- **Solution:**
  - Defer non-critical JavaScript (11 render-blocking scripts found).
  - Preload the LCP image (hero) with `<link rel="preload" as="image">`.
  - Optimize server response time (TTFB is 4 ms, so focus on resource delivery).

1G. Force HTTP to HTTPS Redirect

- **Impact:** Security, Data Integrity
- **Problem:** Security Headers audit confirms http://kawiare.ee/... does not redirect to HTTPS, allowing unencrypted traffic.
- **Solution:** Configure the web server (Apache/Nginx) to return a 301/302 redirect for all HTTP requests to the HTTPS equivalent.

  Apache Example:

  ```
  RewriteEngine On
  RewriteCond %{HTTPS} off
  RewriteRule ^(.*)$ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]
  ```

1H. Defer Render-Blocking JavaScript

- **Impact:** LCP, FCP, Performance
- **Problem:** 11 render-blocking scripts in cause LCP to reach 8.5s and FCP 4.6s on mobile.
- **Solution:** Add `defer` or `async` attributes to non-critical scripts in the `<head>`. Move critical CSS inline and defer the rest.

  Example:

  ```
  <script src="/js/main.js" defer></script>
  ```

1I. Enforce HTTPS Redirect

- **Impact:** Security, Transport Layer
- **Problem:** Security Headers audit reports 'HTTPS redirect: □ http://kawiare.ee... does not redirect to HTTPS'.
- **Solution:** Configure the web server (Apache/Nginx) to return a 301 redirect for all HTTP requests to HTTPS.

  Apache (.htaccess):

  ```
  RewriteEngine On
  RewriteCond %{HTTPS} off
  RewriteRule ^(.*)$ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]
  ```

1J. Optimize Mobile Largest Contentful Paint (LCP)

- **Impact:** Performance, Mobile UX

- **Problem:** Mobile LCP is 9.0s (threshold is 2.5s), driven by render-blocking scripts and heavy assets.
- **Solution:**
  - Defer non-critical JavaScript (11 render-blocking scripts found).
  - Preload the LCP image (hero) with `fetchpriority="high"`.
  - Compress images to WebP/AVIF.
  - Remove unused JavaScript (224KB wasted in `main.js`).

1K. Enforce HTTP to HTTPS redirect

- **Impact:** Security, Transport Layer
- **Problem:** Security Headers audit shows http://kawiare.ee... does not redirect to HTTPS, leaving users vulnerable on unencrypted connections.
- **Solution:** Configure the web server (Apache/Nginx) to return a 301 redirect for all HTTP requests to HTTPS:

```
RewriteEngine On
RewriteCond %{HTTPS} off
RewriteRule ^(.*)$ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]
```

1L. Eliminate render-blocking JavaScript

- **Impact:** LCP, FCP, Performance Score
- **Problem:** PSI mobile LCP is 8.6 s; HTML Inventory shows 11 render-blocking scripts including main.js and jQuery.
- **Solution:** Add `defer` or `async` to non-critical scripts in `<head>`. Critical CSS should be inlined, and JS moved to footer or deferred:

```
<script src="main.js" defer></script>
```

Priority 2: Important

Essential for compliance, user reach, and search visibility.

2A. Strengthen security headers

- **Impact:** Security Grade, XSS/Clickjacking Defense
- **Problem:** Security Headers grade 40/100; missing CSP, COOP, CORP. HSTS lacks preload directive.
- **Solution:** Add missing headers via server config (Apache example):

```
Header set Content-Security-Policy "default-src 'self'; script-src
'self' 'unsafe-inline' https://www.googletagmanager.com"
```

```
Header set Cross-Origin-Opener-Policy "same-origin"
Header set Cross-Origin-Resource-Policy "same-origin"
```

2B. Fix HTML structure and navigation

- **Impact:** SEO, Accessibility
- **Problem:** Page contains 3 `<h1>` elements; missing skip-to-content link; W3C error on `<style>` inside `<div>`.
- **Solution:** Ensure exactly one `<h1>` per page. Add skip link before main content. Move inline styles to external CSS or `<style>` block in `<head>`.

```
<a href="#main-content" class="skip-link">Skip to content</a>
```

2C. Complete Security Header Hardening

- **Impact:** XSS, Clickjacking, Transport Security
- **Problem:** Security Headers grade is 40/100; HSTS lacks preload directive, and CSP is missing entirely.
- **Solution:** Add HSTS preload and a strict CSP. Since signals indicate no auth/payments, a restrictive default-src is safe:

```
Header always set Strict-Transport-Security "max-age=63072000;
includeSubDomains; preload"
Header always set Content-Security-Policy "default-src 'self';
script-src 'self' 'unsafe-inline'
https://www.googletagmanager.com;"
```

2D. Fix Heading Hierarchy and Color Contrast

- **Impact:** WCAG 1.3.1, 1.4.3, SEO
- **Problem:** W3C and axe report h1→h3 skip and serious contrast failure on #cookiescript_accept.
- **Solution:**
  - Insert an h2 between h1 and h3, or change h3 to h2.
  - Increase contrast on `.lead-text` or `#cookiescript_accept` to meet 4.5:1 ratio (e.g., darken text or lighten background).

2E. Defer Render-Blocking Scripts

- **Impact:** FCP, TBT, Mobile Performance
- **Problem:** 11 render-blocking scripts in delay First Contentful Paint (3.62 s) and contribute to long tasks.
- **Solution:** Add `defer` or `async` attributes to non-critical scripts in `<head>`:

```
<script src="..." defer></script>
```

Move critical CSS inline and defer the rest.

2F. Fix Accessibility Violations

- **Impact:** WCAG Compliance, Usability
- **Problem:** 1 serious color-contrast violation (#cookiescript_accept) and 3 moderate landmark violations (duplicate main, missing skip-link).
- **Solution:**
  - Increase contrast ratio for `.cookiescript_accept` to ≥4.5:1.
  - Add `<a href="#main" class="skip-link">Skip to content</a>`.
  - Ensure only one `<main>` or `role="main"` element exists.

2G. Fix Color Contrast on Cookie Buttons

- **Impact:** Accessibility (WCAG 1.4.3)
- **Problem:** axe-core reports 1 serious violation: background and foreground colors on #cookiescript_accept/reject do not meet contrast thresholds.
- **Solution:** Increase contrast ratio to at least 4.5:1 for normal text. Adjust button text color or background color in CSS.

  CSS Example:

```
#cookiescript_accept { color: #333333; background: #ffffff; }
```

2H. Correct Invalid HTML Structure

- **Impact:** SEO, Rendering Consistency
- **Problem:** W3C Validator reports 2 errors: `<style>` not allowed as child of `<div>` and unescaped `<` character.
- **Solution:** Move `<style>` blocks to the `<head>` or use `<template>` if dynamic. Escape special characters like `<` as `<` in text content.

  Fix:

```
<!-- Move style to head -->
<head>
  <style>...</style>
</head>
```

2I. Fix Color Contrast Violation

- **Impact:** Accessibility (WCAG 1.4.3)
- **Problem:** axe-core reports 1 serious violation on `#cookiescript_accept` element.
- **Solution:** Increase text contrast ratio to at least 4.5:1 for the cookie consent button text. Adjust CSS color values or background opacity.

2J. Fix accessibility contrast and landmarks

- **Impact:** WCAG 1.4.3, 2.4.1
- **Problem:** axe-core reports 1 serious color-contrast violation (#cookiescript_accept) and missing skip-to-content link.
- **Solution:**
  - Increase contrast on `.lead-text` and cookie button to ≥4.5:1.
  - Add a skip link at the top of the DOM:

```
<a href="#main" class="skip-link">Otse sisule</a>
```

2K. Strengthen HSTS configuration

- **Impact:** Security Headers Grade
- **Problem:** HSTS is present but missing the `preload` directive, preventing inclusion in browser preload lists.
- **Solution:** Update the `Strict-Transport-Security` header to include preload:

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

2L. Implement Content Security Policy (CSP)

- **Impact:** XSS Defense, Security Headers
- **Problem:** CSP is missing (Security Headers grade 40/100). While site signals show no auth/payments, CSP mitigates XSS risks from third-party scripts (e.g., GTM).
- **Solution:** Deploy a strict CSP with nonce/hash for scripts:

```
Header set Content-Security-Policy "default-src 'self'; script-src
'nonce-{random}' 'strict-dynamic'; style-src 'self' 'unsafe-
inline';"
```

2M. Fix Color Contrast and Landmarks

- **Impact:** Accessibility (WCAG 1.4.3, 1.3.1)

- **Problem:** axe-core found 1 serious color-contrast violation (#cookiescript_accept) and 3 moderate landmark issues (duplicate main).
- **Solution:**
  - Increase contrast on `#cookiescript_accept` to ≥4.5:1.
  - Ensure only one `<main>` element exists; remove duplicate `role="main"`.
  - Add `aria-label` to landmarks if roles are duplicated.

Priority 3: Best Practice

Recommended for long-term maintainability.

3A. Fix color contrast on cookie banner

- **Impact:** WCAG 1.4.3
- **Problem:** axe-core reports serious contrast violation on `#cookiescript_accept`.
- **Solution:** Increase text color contrast ratio to ≥4.5:1 against the background. Verify with a contrast checker tool.

3B. Replace CSS Background Hero with Real Image

- **Impact:** LCP, Image Optimization
- **Problem:** Hero uses CSS background-image, preventing srcset usage and browser optimization; LCP element is heavy.
- **Solution:** Move the hero image into an `<img>` tag with `fetchpriority="high"` and `srcset`:

  ```
  <img src="hero-800.jpg" srcset="hero-400.jpg 400w, hero-800.jpg 800w" fetchpriority="high" alt="...">
  ```

3C. Add Content Security Policy (CSP)

- **Impact:** XSS Defense-in-Depth
- **Problem:** CSP is missing. Site signals indicate no auth/payments/UGC, so risk is lower than P1, but still recommended for defense.
- **Solution:** Implement a strict CSP with nonce/hash for scripts:

  ```
  Header set Content-Security-Policy "default-src 'self'; script-src 'nonce-{random}' 'strict-dynamic';"
  ```

  Ensure all inline scripts use the nonce.

3D. Implement Content Security Policy (CSP)

- **Impact:** XSS Defense-in-Depth

- **Problem:** CSP is missing. Site signals indicate no auth/payments, so this is a best practice rather than critical, but recommended for hardening.
- **Solution:** Deploy a strict CSP with nonces for scripts. Since this is a brochure/blog page, a strict allowlist is feasible.

  Header:

  ```
  Content-Security-Policy: default-src 'self'; script-src 'nonce-{random}' 'strict-dynamic';
  ```

3E. Resolve W3C Validation Errors

- **Impact:** SEO, Rendering Consistency
- **Problem:** 2 errors found: `<style>` not allowed in `div` context and unescaped `<` character in text content.
- **Solution:**
  - Move inline `<style>` blocks to the `<head>` or external CSS file.
  - Escape special characters in text content (e.g., use `&lt;` instead of `<`).

3F. Add Meta Description

- **Impact:** SEO, Click-Through Rate
- **Problem:** W3C and SEO audits confirm the document lacks a meta description.
- **Solution:** Add a concise description (150–160 chars) in the `<head>`:

  ```
  <meta name="description" content="Ahven ja koha – kaks Balti järvede kala, mille väärtus vajab uuesti mõtestamist.">```
  ```

3G. Add Security Headers (CSP, HSTS Preload)

- **Impact:** Defense-in-depth, Security Score
- **Problem:** CSP is missing; HSTS lacks preload directive. Site signals indicate low auth/payment risk, so this is P3.
- **Solution:** Add CSP with nonce/hash strategy. Add `preload` to HSTS.

  Apache:

  ```
  Header set Strict-Transport-Security "max-age=63072000; includeSubDomains; preload"
  Header set Content-Security-Policy "default-src 'self'; script-src 'nonce-{random}' 'strict-dynamic'"
  ```

3H. Improve SEO and Validation

- **Impact:** Search Visibility, Code Quality
- **Problem:** Missing meta description; W3C validator reports 2 errors (invalid `<style>` in `<div>`, unescaped `<`).
- **Solution:**
  - Add `<meta name="description" content="...">`.
  - Fix W3C errors: Move `<style>` blocks to `<head>` or use `<div>` correctly; escape `<` as `&lt;`.

3I. Improve SEO and HTML Validity

- **Impact:** Search Visibility, Code Quality
- **Problem:** PSI SEO audit fails `metaDescription`; W3C reports 2 errors (invalid `<style>` in `div`, unescaped `<` character).
- **Solution:**
  - Add `<meta name="description" content="...">`.
  - Fix W3C errors: move `<style>` to `<head>` or use `<div>` correctly; escape `<` as `&lt;` in text content.