Audit Report: Perfectly formed web development team - gotoAndPlay

Website: https://play.ee/
Date: 15.09.2026
Audit Coverage: 100% — all sources returned data
Confidence: high

Pages Audited (5 of 5):

- https://play.ee/
- https://play.ee/web-development-case-studies/
- https://play.ee/software-development-work-index/
- https://play.ee/wordpress-support-service/
- https://play.ee/web-development-in-estonia/

Summary of results

Overall Score: 75 / 100
Status: Needs Improvement

Site overall 75 is the mean of 5 pages. Scores range 72 (https://play.ee/software-development-work-index/) → 78 (https://play.ee/). Weakest page: PSI mobile performance is strong at 91, but the Security Headers grade of 20/100 and missing HTTP-to-HTTPS redirect create critical exposure regardless of site signals. W3C validation shows 7 errors including a parser recovery failure, and axe-core flags 1 serious contrast violation alongside missing landmarks. Image assets lack dimensions (53 images), risking CLS regression despite the current 0.039 score. Confidence is high due to complete tool coverage and consistent signals.

Per-page scores

 Needs Improvement · https://play.ee/

Score	Performance	Accessibility	Best Practices	SEO	Security
78	95	100	100	92	20

 Needs Improvement · https://play.ee/web-development-case-studies/

Score	Performance	Accessibility	Best Practices	SEO	Security
75	95	90	96	100	20

 Needs Improvement · https://play.ee/software-development-work-index/

Score	Performance	Accessibility	Best Practices	SEO	Security
72	91	90	96	100	20

 Needs Improvement · https://play.ee/wordpress-support-service/

Score	Performance	Accessibility	Best Practices	SEO	Security
72	96	91	100	100	20

 Needs Improvement · https://play.ee/web-development-in-estonia/

Score	Performance	Accessibility	Best Practices	SEO	Security
76	96	94	100	100	20

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://play.ee/	**95** / 100	**2.51 s** / 547 ms	0.001 / **0.005**
https://play.ee/web-development-case-studies/	**95** / 99	**2.57 s** / 582 ms	0.005 / **0.005**
https://play.ee/software-development-work-index/	**91** / 100	**2.48 s** / 540 ms	**0.039** / 0.004
https://play.ee/wordpress-support-service/	**96** / 100	**2.35 s** / 580 ms	**0.017** / 0.001
https://play.ee/web-development-in-estonia/	96 / 96	**2.40 s** / 555 ms	0.002 / **0.005**

Optimization Checklist

2 of 2 passing — 2 pass · 0 warn · 0 fail · 5 n/a

Item	Status	Detail
Page caching plugin / CDN active	**Pass**	Caching plugin detected (WP Rocket)
Images lazy-loaded	N/A	No raster elements found (37 SVGs, 13 placeholders excluded).
Hero image eagerly loaded	N/A	No raster elements found (37 SVGs, 13 placeholders excluded).
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 0 raster images on the page (37 SVGs, 13 placeholders excluded) — 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. Enforce HTTPS and add baseline security headers `Security`

- **Impact:** Transport security, clickjacking, MIME sniffing
- **Problem:** Security Headers grade is 20/100; HTTP does not redirect to HTTPS, and HSTS, X-Content-Type-Options are missing.
- **Solution:** Configure server to redirect all HTTP traffic to HTTPS (301). Add these headers:

```
Strict-Transport-Security: max-age=63072000; includeSubDomains
X-Content-Type-Options: nosniff
```

```
X-Frame-Options: SAMEORIGIN
```

1B. Force HTTPS redirect and add HSTS `Security`

- **Impact:** Transport security, MITM protection
- **Problem:** HTTP does not redirect to HTTPS and HSTS is missing (Security Headers grade 20/100).
- **Solution:** Configure server to redirect all HTTP traffic to HTTPS (301) and send HSTS header:

```
Header always set Strict-Transport-Security "max-age=63072000;
includeSubDomains; preload"
RewriteEngine On
RewriteCond %{HTTPS} off
RewriteRule ^(.*)$ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]
```

1C. Fix W3C HTML Validation Errors `SEO`

- **Impact:** Rendering consistency, SEO indexing
- **Problem:** 7 errors including parser recovery failure at line 100; iframe/noscript in head is invalid.
- **Solution:** Move `<noscript><iframe>` block out of `<head>` or use valid placement. Fix meta tag attributes (`name` vs `property`). Ensure `<body>` opens after `<head>` closes properly.

1D. Enforce HTTPS redirect and add HSTS `Security`

- **Impact:** Transport security, MITM protection
- **Problem:** HTTP does not redirect to HTTPS (Security Headers finding) and HSTS is missing, leaving initial requests vulnerable.
- **Solution:** Configure server to redirect all HTTP traffic to HTTPS (301) and send HSTS header:

```
Header always set Strict-Transport-Security "max-age=63072000;
includeSubDomains; preload"
RewriteCond %{HTTPS} off
RewriteRule ^(.*)$ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]
```

1E. Add X-Content-Type-Options and X-Frame-Options `Security`

- **Impact:** MIME sniffing, clickjacking
- **Problem:** X-Content-Type-Options and X-Frame-Options are missing (Security Headers grade 20/100).
- **Solution:** Add these headers to all responses:

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

1F. Enforce HTTPS and add HSTS `Security`

- **Impact:** Transport security, data integrity
- **Problem:** HTTP does not redirect to HTTPS and HSTS is missing (Security Headers grade 20/100).
- **Solution:** Configure server to redirect all HTTP traffic to HTTPS and add HSTS header:

```
RewriteEngine On
RewriteCond %{HTTPS} off
RewriteRule ^(.*)$ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]
Header always set Strict-Transport-Security "max-age=63072000;
includeSubDomains; preload"
```

1G. Fix contrast and link names `Accessibility`

- **Impact:** WCAG 1.4.3, 2.4.4 compliance
- **Problem:** 2 serious axe violations: color-contrast on `.button--tertiary` and link-name on logo links.
- **Solution:**
  - Increase contrast ratio for `.button--tertiary` text to ≥4.5:1.
  - Add `aria-label` to logo links (e.g., `<a aria-label="Client Logo">`).

1H. Force HTTPS Redirect `Security`

- **Impact:** Transport security, data integrity
- **Problem:** HTTP does not redirect to HTTPS (http://play.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]
```

Priority 2: Important

Essential for compliance, user reach, and search visibility.

2A. Fix W3C HTML validation errors `SEO`

- **Impact:** Parser recovery, document structure
- **Problem:** W3C Validator reports 7 errors including 'Cannot recover after last error' at line 101 and invalid iframe/noscript placement in head.
- **Solution:** Move `<noscript><iframe>` tags out of the `<head>` section. Ensure all `<meta>` tags are valid and remove stray end tags. Fix the parser recovery issue to ensure full document parsing.

2B. Add skip link and main landmark `Accessibility`

- **Impact:** Keyboard navigation, screen reader flow
- **Problem:** HTML Inventory shows 'main' landmark missing and no skip-to-content link; axe-core flags 'region' violations.
- **Solution:** Add a skip link at the top of the page:

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

  Wrap primary content in `<main id="main-content">`.

2C. Fix Color Contrast and Add Main Landmark `Accessibility`

- **Impact:** WCAG 1.4.3, 1.3.1
- **Problem:** 1 serious axe violation on color-contrast (h1, cards); Document lacks `main` landmark.
- **Solution:**
  - Increase text contrast to ≥4.5:1 (e.g., darken `#heading__main`).
  - Wrap primary content in `<main>` tag.
  - Add `<a href="#content" class="skip-link">Skip to content</a>`.

2D. Add Image Dimensions and Lazy Loading `Performance`

- **Impact:** CLS, LCP
- **Problem:** 56 images missing width/height attributes and lazy loading (CLS risk).
- **Solution:** Add `width` and `height` attributes to all `<img>` tags. Add `loading="lazy"` to images below the fold:

  ```
  <img src="..." alt="..." width="300" height="200" loading="lazy">
  ```

2E. Add explicit width and height to images `Performance`

- **Impact:** CLS, Layout stability

- **Problem:** HTML Inventory shows 53 images without width/height attributes, risking CLS despite current 0.039 score.
- **Solution:** Add `width` and `height` attributes to all `<img>` tags:

```
<img src="image.jpg" alt="..." width="800" height="600">
```

2F. Fix HTML structure and headings `SEO`

- **Impact:** Document outline, W3C validation
- **Problem:** 7 W3C errors (malformed `<head>` / `<body>`) and 2 `<h1>` elements found.
- **Solution:**
  - Ensure only one `<h1>` per page.
  - Fix `<noscript>` injection in `<head>` (likely GTM/Plugin issue).
  - Add `<main>` landmark wrapping primary content.

2G. Eliminate render-blocking resources `Performance`

- **Impact:** FCP, LCP, Time to Interactive
- **Problem:** Render-blocking insight estimates 990 ms savings; unused CSS (31 KiB) and JS (23 KiB) detected.
- **Solution:**
  - Defer non-critical CSS.
  - Inline critical CSS.
  - Remove unused JS/CSS rules via build process or plugin settings.

2H. Add HSTS and X-Content-Type-Options `Security`

- **Impact:** Protocol downgrade protection, MIME sniffing
- **Problem:** HSTS and X-Content-Type-Options headers are missing (Security Headers grade 20/100).
- **Solution:** Add these headers to the server response.

  Apache:

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

2I. Resolve W3C HTML Validation Errors `Best Practices`

- **Impact:** DOM parsing, SEO, rendering stability

- **Problem:** 7 validation errors including parser recovery failure at line 100 (W3C Validator).
- **Solution:** Fix the `<noscript>` iframe placement in `<head>` and remove stray end tags.
  - Move Google Tag Manager `<noscript>` iframe to `<body>`.
  - Ensure `<meta>` tags do not use invalid `name` attributes in this context.
  - Validate the document structure after changes.

Priority 3: Best Practice

Recommended for long-term maintainability.

3A. Eliminate render-blocking resources `Performance`

- **Impact:** FCP, LCP
- **Problem:** PageSpeed Insights flags 1 render-blocking script and 30 KiB unused CSS; LCP is 2.5 s.
- **Solution:** Defer non-critical scripts. Inline critical CSS or use `preload` for critical stylesheets. Remove unused CSS rules identified in the audit.

3B. Add explicit dimensions to images `Best Practices`

- **Impact:** CLS, Layout stability
- **Problem:** HTML Inventory shows 50 images missing width/height attributes, which can cause layout shifts despite current CLS of 0.001.
- **Solution:** Add `width` and `height` attributes to all `<img>` tags. For SVGs, use `viewBox` and CSS aspect-ratio if intrinsic dimensions are not available.

3C. Strengthen Content Security Policy `Security`

- **Impact:** XSS defense-in-depth
- **Problem:** CSP is weak (only `frame-ancestors`); site signals show no auth/payments, so P3 per rubric.
- **Solution:** If adding forms or user content later, deploy a nonce-based CSP:

```
Header always set Content-Security-Policy "default-src 'self';
script-src 'nonce-{random}' 'strict-dynamic'; object-src 'none';"
```

3D. Implement Content-Security-Policy (CSP) `Security`

- **Impact:** XSS defense-in-depth
- **Problem:** CSP is missing or weak (only frame-ancestors). Site signals show no auth/payments, so this is P3 per rubric.

- **Solution:** Deploy a nonce-based CSP when ready:

```
Header always set Content-Security-Policy "default-src 'self';
script-src 'nonce-{random}' 'strict-dynamic'; object-src 'none';
base-uri 'none';"
```

3E. Implement Content Security Policy `Security`

- **Impact:** XSS defense-in-depth
- **Problem:** CSP is missing (only `frame-ancestors` set). Site signals show no auth/payments/UGC.
- **Solution:** Add a restrictive CSP header. Since this is a brochure site, start with a strict default-src:

```
Header always set Content-Security-Policy "default-src 'self';
script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-
inline';"
```

3F. Add Image Dimensions and Lazy Loading `Performance`

- **Impact:** CLS, Initial Load
- **Problem:** 67 images missing explicit width/height and `loading="lazy"` (HTML Inventory).
- **Solution:** Add `width` and `height` attributes to all `<img>` tags to reserve space. Add `loading="lazy"` to images below the fold.

```
<img src="image.jpg" alt="..." width="300" height="200"
loading="lazy">
```