Audit Report: Perfectly formed web development team - gotoAndPlay

Website: https://play.ee/
Date: 24.09.2026
Audit Coverage: 100% — all sources returned data
Confidence: high

Pages Audited (1 of 1):

- https://play.ee/

Summary of results

Overall Score: 78 / 100
Status: **Needs Improvement**

PSI mobile 97 indicates excellent performance (LCP 2.3 s, CLS 0.001), but the Security basics verdict is FAILED. Per the audit protocol: 'Treat FAILED as a must-fix and PASS as a starting point, not a certificate.' W3C validation returned 7 errors including parser recovery failure, and accessibility has 2 moderate violations plus missing landmarks. Image assets lack width/height attributes on all 50 images, risking future CLS. These structural and security hygiene issues prevent a higher score despite the fast load times.

Per-page scores

 Needs Improvement · https://play.ee/

Score	Performance	Accessibility	Best Practices	SEO	Security
78	97	94	100	92	FAILED

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	**97** / 100	**2.33 s** / 588 ms	0.001 / **0.007**

Optimization Checklist

3 of 3 passing — 3 pass · 0 warn · 0 fail · 5 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	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. Fix HTTP redirect and add baseline security headers `Security`

- **Impact:** Transport security, clickjacking, MIME sniffing

- **Problem:** Security basics verdict is FAILED: http:// does not redirect to https, HSTS is missing, and X-Content-Type-Options is missing.
- **Solution:** Configure server to redirect HTTP to HTTPS and send these headers:

```
Header always set Strict-Transport-Security "max-age=63072000;
includeSubDomains"
Header always set X-Content-Type-Options "nosniff"
Redirect permanent / https://play.ee/
```

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 reported 7 errors including 'Cannot recover after last error' at line 101 and bad iframe/noscript nesting in head.
- **Solution:** Move `<noscript><iframe>...</iframe></noscript>` out of `<head>` or ensure it is valid HTML5. Remove stray end tags and fix meta tag attributes (e.g., `name` vs `property`).

2B. Add skip-to-content link and fix landmarks `Accessibility`

- **Impact:** Keyboard navigation, screen reader flow
- **Problem:** axe-core found `landmark-unique` and `region` violations; HTML inventory confirms missing `main` landmark and skip link.
- **Solution:** Add a skip link at the top of the body:

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

  Wrap main content in `<main id="main-content">` and ensure nav/footer have unique labels.

2C. Add width and height to all images `Performance`

- **Impact:** CLS (Cumulative Layout Shift)
- **Problem:** HTML inventory shows 50 images without explicit width/height attributes, risking layout shifts despite current CLS of 0.001.
- **Solution:** Add `width` and `height` attributes to all `<img>` tags matching their intrinsic dimensions. For responsive images, use `srcset` with corresponding sizes.

2D. Harden WordPress installation `Security`

- **Impact:** Brute-force protection, attack surface
- **Problem:** Security basics flagged `xmlrpc.php` accepts POST requests and `/wp-admin/install.php` is reachable.
- **Solution:** Disable xmlrpc.php in .htaccess or via plugin. Block access to `/wp-admin/install.php` after installation:

```
<Files install.php>
  Order Allow,Deny
  Deny from all
</Files>
```

Priority 3: Best Practice

Recommended for long-term maintainability.

No items.