Audit Report: Full-stack digital solutions – premier custom software & design

Website: https://playandnope.com/
Date: 09.10.2026
Audit Coverage: 96% — PageSpeed Insights (mobile): PSI HTTP 500; PageSpeed Insights (desktop): PSI HTTP 500
Confidence: medium

Pages Audited (5 of 5):

- https://playandnope.com/
- https://playandnope.com/privacy-policy
- https://playandnope.com/contact
- https://playandnope.com/digital-solutions-contact
- https://playandnope.com/digiagentuur-klientide-tagasiside

Summary of results

Overall Score: 73 / 100
Status: □ □ **Needs Improvement**

Site overall 73 is the mean of 5 pages. Scores range 55 (https://playandnope.com/digital-solutions-contact) → 88 (https://playandnope.com/digiagentuur-klientide-tagasiside). Weakest page: Performance is catastrophically low (PSI Mobile 35, LCP 11.1 s, TBT 24.77 s), dragging the overall score into the 'Poor' band despite excellent Accessibility (99) and SEO (100). The site signals indicate User-Generated Content (textarea), elevating CSP importance, though the Security basics verdict is PASS. TTFB is excellent (45 ms), but client-side JavaScript execution blocks the main thread for over 24 seconds. Confidence is medium because PSI Desktop failed (HTTP 500), forcing mobile data duplication.

Per-page scores

□ **Needs Improvement** · https://playandnope.com/

Score	Performance	Accessibility	Best Practices	SEO	Security
78	67	100	100	92	PASS

 Needs Improvement · https://playandnope.com/privacy-policy

Score	Performance	Accessibility	Best Practices	SEO	Security
86	94	100	100	100	PASS

 Poor · https://playandnope.com/contact

Score	Performance	Accessibility	Best Practices	SEO	Security
58	34	99	96	100	PASS

 Poor · https://playandnope.com/digital-solutions-contact

Score	Performance	Accessibility	Best Practices	SEO	Security
55	35	99	96	100	PASS

 Needs Improvement · https://playandnope.com/digiagentuur-klientide-tagasiside

Score	Performance	Accessibility	Best Practices	SEO	Security
88	92	100	100	100	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://playandnope.com/	— / 67	— / 486 ms	— / 0.084
https://playandnope.com/privacy-policy	94 / **82**	**2.13 s** / 567 ms	0.100 / **0.365**
https://playandnope.com/contact	34 / —	9.86 s / —	0.055 / —

URL	Performance (M / D)	LCP (M / D)	CLS (M / D)
https://playandnope.com/digital-solutions-contact	35 / —	11.10 s / —	0.056 / —
https://playandnope.com/digiagentuur-klientide-tagasiside	**92** / 97	**2.23 s** / 598 ms	**0.129** / 0.084

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 (25 SVGs, 5 placeholders excluded).
Hero image eagerly loaded	N/A	No raster elements found (25 SVGs, 5 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 (25 SVGs, 5 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. Reduce Main Thread Blocking Time (TBT) `Performance`

- **Impact:** TBT, Interactive, FID
- **Problem:** TBT is 25,150 ms and Interactive is 33.8 s, caused by long tasks in global.js (multiple 300–550 ms tasks).
- **Solution:**
  - Split `global.js` into smaller chunks loaded after interaction.
  - Defer non-critical JS execution until idle.
  - Investigate WebGL GPU stall warnings in console which may contribute to main thread contention.

1B. Fix h1 color contrast `Accessibility`

- **Impact:** WCAG 1.4.3 compliance
- **Problem:** axe-core reports 1 serious violation: color-contrast on the h1 element.
- **Solution:** Increase the contrast ratio between the h1 text and background to at least 4.5:1. Use a color picker tool to verify the hex values meet WCAG AA standards.

1C. Reduce JavaScript execution time and blocking `Performance`

- **Impact:** TBT, LCP, FCP
- **Problem:** TBT is 23.28 s and LCP is 9.9 s; unused JS includes ~170 KB reCAPTCHA and ~92 KB theme global.js.
- **Solution:**
  - Defer non-critical scripts (reCAPTCHA) until user interaction.
  - Code-split theme JS (`global.js` , `jquery.min.js`) to remove unused code.
  - Consider lazy-loading reCAPTCHA only when the form is scrolled into view.

1D. Reduce JavaScript execution time and unused code `Performance`

- **Impact:** TBT, LCP, FCP
- **Problem:** TBT is 24.77 s and LCP is 11.1 s due to 1.16 MB of scripts, including 176 KB of unused reCAPTCHA JS and multiple long tasks in theme JS.
- **Solution:**

    - Defer non-critical scripts (e.g., reCAPTCHA) until user interaction.
    - Remove unused JavaScript (176 KB wasted in reCAPTCHA, 92 KB in theme JS).
    - Split code bundles to reduce main thread blocking.
    - Use `requestIdleCallback` for non-essential initialization.

1E. Harden Content-Security-Policy (CSP) `Security`

- **Impact:** XSS protection, UGC safety
- **Problem:** CSP is present but weak (missing `default-src`, `object-src 'none'`). Site has UGC (textarea), increasing XSS risk per rubric.
- **Solution:**
    - Add `default-src 'self'` to restrict resource loading.
    - Add `object-src 'none'` to block Flash/objects.
    - Use nonce-based CSP for scripts: `script-src 'nonce-{random}' 'strict-dynamic'`.
    - Ensure `frame-ancestors 'self'` remains.

1F. Fix color contrast on navigation descriptions `Accessibility`

- **Impact:** WCAG 1.4.3 compliance, screen reader usability
- **Problem:** axe-core reports 1 serious violation on `.menu-item-74 > .navigation__description` and `.menu-item-75`.
- **Solution:** Increase text contrast ratio to at least 4.5:1 against the background. Adjust CSS:

```
.menu-item-74 .navigation__description, .menu-item-75
.navigation__description {
  color: #333333; /* Example darker shade */
}
```

Priority 2: Important

Essential for compliance, user reach, and search visibility.

2A. Disambiguate Vague Link Text `SEO`

- **Impact:** Link Text, Accessibility
- **Problem:** HTML inventory found 4 instances of 'read more' and repeated generic text like 'business transformation' without context.
- **Solution:**

- Replace generic link text with descriptive targets, e.g., `<a href="/services">Read more about our services</a>`.
- Use `aria-label` if visual text must remain generic.

2B. Add Explicit Image Dimensions `Performance`

- **Impact:** CLS, Layout Stability
- **Problem:** 5 images lack width/height attributes, risking layout shifts despite current CLS of 0.084.
- **Solution:**
  - Ensure all `<img>` tags include `width` and `height` attributes matching intrinsic dimensions.
  - Use CSS aspect-ratio if dimensions are dynamic.

2C. Reduce unused JavaScript `Performance`

- **Impact:** Page weight, TBT
- **Problem:** 112 KB of unused JavaScript found in global.min.js (approx. 50% of total script weight).
- **Solution:** Audit `global.62444fa2566b44750ca1.min.js` to identify unused functions. Consider code splitting or removing legacy polyfills not needed for modern browsers.

2D. Stabilize layout shifts `Performance`

- **Impact:** CLS score
- **Problem:** Mobile CLS is 0.100 (warning threshold); shift source identified in `div.cm` within the privacy policy content.
- **Solution:** Ensure dynamic content (e.g., cookie consent banners or embedded iframes) reserves space before loading. Add explicit dimensions to any injected elements.

2E. Strengthen Content-Security-Policy (CSP) `Security`

- **Impact:** XSS defense for form input
- **Problem:** CSP is present but weak: missing `default-src` and `object-src 'none'`; site has a textarea (UGC signal).
- **Solution:** Add strict directives to the CSP header:

```
Content-Security-Policy: default-src 'self'; object-src 'none';
script-src 'self' 'nonce-{random}' https://www.gstatic.com; frame-
ancestors 'self';
```

Ensure nonce is rotated per request.

2F. Label the contact form textarea `Accessibility`

- **Impact:** WCAG 1.3.1, 3.3.2
- **Problem:** HTML Inventory shows 1 textarea with no label; screen readers cannot identify the field.
- **Solution:** Add a visible `<label>` element or `aria-label` to the textarea:

```
<label for="message">Your Message</label>
<textarea id="message" name="message"></textarea>
```

2G. Label form textarea and hidden inputs `Accessibility`

- **Impact:** WCAG 1.3.1, 3.3.2
- **Problem:** HTML Inventory shows a textarea with no label; W3C reports 2 errors on hidden inputs with autocomplete attributes.
- **Solution:**
  - Add `<label for="...">` to the textarea or use `aria-label`.
  - Remove `autocomplete` attribute from `<input type="hidden">` elements (W3C error).
  - Ensure all form fields have associated labels for screen readers.

2H. Reduce Cumulative Layout Shift (CLS) `Performance`

- **Impact:** Visual stability, Core Web Vitals score
- **Problem:** Mobile CLS is 0.129 (warning threshold >0.1); shift sources identified in `.cm-wrapper` and `.hero`.
- **Solution:** Reserve space for dynamic content or images. Ensure fonts do not cause layout shifts (use `font-display: swap` with fallback metrics). Add explicit `width` and `height` attributes to all media elements.

2I. Eliminate unused JavaScript `Performance`

- **Impact:** Page weight, FCP, TBT
- **Problem:** 112 KB wasted in `global.62444fa2566b44750ca1.min.js` (unused JS finding).
- **Solution:** Audit the `global` script for unused functions. Consider code splitting or tree-shaking to remove dead code. If using WordPress, disable unused theme scripts via a performance plugin.

Priority 3: Best Practice

Recommended for long-term maintainability.

3A. Harden Content Security Policy `Security`

- **Impact:** XSS Defense
- **Problem:** CSP is present but weak: missing `default-src` and `object-src 'none'`. Site signals indicate no auth/payments, so risk is lower.
- **Solution:**
  - Add `default-src 'self'` and `object-src 'none'` to the CSP header.
  - Example: `Content-Security-Policy: default-src 'self'; object-src 'none'; frame-ancestors 'self';`

3B. Add Cross-Origin Headers `Security`

- **Impact:** Data Leakage, Isolation
- **Problem:** COOP and CORP headers are missing; Server header discloses Apache.
- **Solution:**
  - Add `Cross-Origin-Opener-Policy: same-origin`.
  - Add `Cross-Origin-Resource-Policy: same-origin`.
  - Consider removing `Server: Apache` header via server config.

3C. Harden Content-Security-Policy `Security`

- **Impact:** XSS defense-in-depth
- **Problem:** CSP is present but weak: missing `default-src` and `object-src 'none'`; only `frame-ancestors` is set.
- **Solution:** Since the site has no auth or payments (low risk), a strict CSP is optional but recommended. Add `default-src 'self'` and `object-src 'none'` to the existing header.

3D. Add Subresource Integrity (SRI) `Security`

- **Impact:** Script tampering protection
- **Problem:** 2 cross-origin scripts (jsdelivr) lack integrity attributes.
- **Solution:** Add `integrity` and `crossorigin` attributes to external script tags. Example: `<script src="..." integrity="sha384-..." crossorigin="anonymous"></script>`.

3E. Add Subresource Integrity (SRI) and COOP/CORP `Security`

- **Impact:** Supply chain security, context isolation

- **Problem:** 3 of 4 cross-origin scripts lack integrity attributes; COOP and CORP headers are missing.
- **Solution:**
  - Add `integrity` and `crossorigin` attributes to external script tags (e.g., reCAPTCHA, CDN scripts).
  - Add headers:

```
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
```

3F. Add Cross-Origin headers and hide server version `Best Practices`

- **Impact:** COOP, CORP, Info Disclosure
- **Problem:** COOP and CORP headers are missing; Server header discloses 'Apache'.
- **Solution:**
  - Add `Cross-Origin-Opener-Policy: same-origin`.
  - Add `Cross-Origin-Resource-Policy: same-origin`.
  - Configure server to suppress `Server` header or set to generic value.

3G. Harden Content-Security-Policy (CSP) `Security`

- **Impact:** XSS defense-in-depth
- **Problem:** CSP is present but weak: missing `default-src` and `object-src 'none'`.
- **Solution:** Define a strict policy. Since this is a brochure site (no auth/UGC), a restrictive allowlist is safe:

```
Content-Security-Policy: default-src 'self'; object-src 'none';
base-uri 'self'; form-action 'self';
```

3H. Enable HSTS Preload and COOP/CORP `Security`

- **Impact:** Transport security, context isolation
- **Problem:** HSTS lacks preload directive; COOP and CORP headers are missing.
- **Solution:** Add `preload` to HSTS and set isolation headers:

```
Strict-Transport-Security: max-age=31536000; includeSubDomains;
preload
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
```