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

Website: https://playandnope.com/
Date: 06.10.2026
Audit Coverage: 98% — PageSpeed Insights (desktop): PSI HTTP 500; PageSpeed Insights (desktop): PSI HTTP 502
Confidence: medium

Pages Audited (5 of 5):

- https://playandnope.com/
- https://playandnope.com/privacy-policy
- https://playandnope.com/contact
- https://playandnope.com/design-service
- https://playandnope.com/digiagentuur-klientide-tagasiside

Summary of results

Overall Score: 67 / 100
Status: □ □ **Needs Improvement**

Site overall 67 is the mean of 5 pages. Scores range 50 (https://playandnope.com/contact) → 76 (https://playandnope.com/digiagentuur-klientide-tagasiside). Weakest page: Performance is catastrophic with a PSI mobile score of 33, LCP of 12.4 s, and TBT of 24.9 s, dragging the score heavily into the 'Poor' band. Security basics FAILED due to missing HSTS and X-Content-Type-Options, and WordPress hygiene issues (xmlrpc.php open) further reduce trust. Accessibility is moderate with 5 violations including missing main landmark and heading skips, though no critical/serious issues were found. Desktop PSI data was unavailable (HTTP 502), so mobile metrics were used for both, slightly lowering confidence. Image assets are mostly SVGs with lazy loading, which is positive, but JS bloat (1.16 MB) is the primary performance blocker.

Per-page scores

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

Score	Performance	Accessibility	Best Practices	SEO	Security
62	64	96	100	85	FAILED

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

Score	Performance	Accessibility	Best Practices	SEO	Security
72	75	98	100	92	FAILED

 Poor · https://playandnope.com/contact

Score	Performance	Accessibility	Best Practices	SEO	Security
50	33	98	96	92	FAILED

 Needs Improvement · https://playandnope.com/design-service

Score	Performance	Accessibility	Best Practices	SEO	Security
74	93	95	100	92	FAILED

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

Score	Performance	Accessibility	Best Practices	SEO	Security
76	84	100	100	92	FAILED

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/	64 / —	1.96 s / —	0.089 / —
https://playandnope.com/privacy-policy	**75** / 98	**6.59 s** / 544 ms	0.000 / **0.084**
https://playandnope.com/contact	33 / —	12.41 s / —	0.083 / —

URL	Performance (M / D)	LCP (M / D)	CLS (M / D)
https://playandnope.com/design-service	**93** / 96	**2.25 s** / 615 ms	0.087 / **0.098**
https://playandnope.com/digiagentuur-klientide-tagasiside	**84** / 94	**4.12 s** / 624 ms	0.040 / **0.136**

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 (18 SVGs, 12 placeholders excluded).
Hero image eagerly loaded	N/A	No raster elements found (18 SVGs, 12 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 (18 SVGs, 12 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 Total Blocking Time (TBT) from 22,350 ms `Performance`

- **Impact:** Interactivity, TBT, Time to Interactive
- **Problem:** TBT is 22,350 ms with multiple long tasks (>200 ms) in global.620687d605be8ba84f0e.min.js and core.c872dceb075db34864df.min.js.
- **Solution:**
  - Split large JavaScript bundles using code splitting.
  - Defer non-critical JS execution until idle.
  - Remove unused JavaScript (92 KB identified).
  - Consider moving heavy logic to Web Workers if applicable.

1B. Add HSTS and X-Content-Type-Options headers `Security`

- **Impact:** Transport security, MIME sniffing protection
- **Problem:** Security basics verdict is FAILED; Strict-Transport-Security and X-Content-Type-Options are missing.
- **Solution:** Add to server configuration (Apache example):

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

1C. Reduce Largest Contentful Paint (LCP) to under 2.5 s `Performance`

- **Impact:** Mobile Performance Score, User Perception
- **Problem:** Mobile LCP is 6.6 s (heavy penalty), driven by 112 KB unused JavaScript and long tasks (105 ms).
- **Solution:**
  - Remove or defer the 112 KB unused JS (`global.620687d605be8ba84f0e.min.js`).
  - Preload critical fonts and ensure hero content is not delayed by layout shifts.
  - Use `renderless` or `priority-hint` attributes for non-critical resources.

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

- **Impact:** TBT, LCP, FCP

- **Problem:** TBT is 24.9 s and LCP is 12.4 s; 1.16 MB of scripts including heavy reCAPTCHA and theme JS cause long tasks (832 ms, 575 ms).
- **Solution:**
  - Defer non-critical JS (e.g., analytics, chat widgets) until user interaction.
  - Optimize reCAPTCHA: load only on form focus or use invisible v3.
  - Split theme JS bundles; remove unused code (92 KB wasted in global.js).
  - Use `render-blocking` resource hints only for critical CSS.

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

- **Impact:** XSS defense
- **Problem:** CSP is weak (missing default-src, object-src); site has user-generated content (textarea), increasing XSS risk per the security rubric.
- **Solution:** Implement a strict CSP with nonce/hash:

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

  Ensure all inline scripts use the nonce.

1F. Optimize image delivery (4 MB total weight) `Performance`

- **Impact:** Page weight, LCP, Speed Index
- **Problem:** Browser Runtime reports 4.03 MB of images out of 4.29 MB total; PSI estimates 4,055 KiB savings potential.
- **Solution:**
  - Convert raster images to WebP/AVIF.
  - Add explicit `width` and `height` attributes to all 25 images to prevent CLS.
  - Implement `srcset` for responsive delivery.

1G. Reduce Largest Contentful Paint (LCP) to under 2.5s `Performance`

- **Impact:** Core Web Vitals, Mobile Performance Score
- **Problem:** Mobile LCP is 4.1s (threshold >4s heavy penalty) despite 9ms TTFB; forced reflow and legacy JS insights indicate render path issues.
- **Solution:**
  - Audit the LCP element (likely hero image or text) and ensure it loads early.
  - Defer non-critical CSS/JS.
  - Preload critical resources.

- Check for layout shifts delaying paint (CLS 0.04 is good, but forced reflow insight suggests paint blocking).

Priority 2: Important

Essential for compliance, user reach, and search visibility.

2A. Add main landmark and fix list structure `Accessibility`

- **Impact:** Screen reader navigation, WCAG 1.3.1, 1.3.2
- **Problem:** axe-core reports missing `<main>` landmark and serious violation on `<ul>` containing non-`<li>` elements.
- **Solution:**
  - Wrap primary content in `<main id="main">`.
  - Ensure `<ul>` and `<ol>` only contain `<li>` elements directly.
  - Add `role="main"` if semantic `<main>` is not used.

2B. Harden WordPress endpoints (xmlrpc.php, install.php) `Security`

- **Impact:** Brute-force protection, installation security
- **Problem:** Security basics flagged xmlrpc.php accepts POST requests and /wp-admin/install.php is reachable.
- **Solution:** Block in .htaccess:

```
<Files xmlrpc.php>
  Order deny,allow
  Deny from all
</Files>

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

2C. Add baseline security headers (HSTS, X-Content-Type-Options) `Security`

- **Impact:** Transport Security, MIME Sniffing Protection
- **Problem:** Security basics verdict is FAILED; HSTS and X-Content-Type-Options are missing despite HTTPS being active.
- **Solution:** Add to server configuration (Apache example):

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

2D. Fix heading hierarchy and add main landmark `Accessibility`

- **Impact:** Screen Reader Navigation, SEO Structure
- **Problem:** Heading order skips from h1 to h3; document lacks a `<main>` landmark (4 axe violations total).
- **Solution:**
  - Change the first `<h3>` after the `<h1>` to `<h2>`.
  - Wrap the primary content in `<main id="main">`.
  - Add a skip-to-content link at the top of the page.

2E. Disable XML-RPC POST requests and block install.php `Security`

- **Impact:** Brute-force Protection, CMS Hardening
- **Problem:** WordPress `xmlrpc.php` accepts POST requests (brute-force vector); `/wp-admin/install.php` is reachable.
- **Solution:** Add to `.htaccess`:

```
<Files xmlrpc.php>
  <Limit POST>
    deny from all
  </Limit>
</Files>
RewriteRule ^wp-admin/install.php - [F,L]
```

2F. Harden WordPress installation `Security`

- **Impact:** Brute-force protection, info disclosure
- **Problem:** xmlrpc.php accepts POST requests (brute-force vector); /wp-admin/install.php is reachable; Server header discloses Apache.
- **Solution:**
  - Block xmlrpc.php in .htaccess or via plugin.
  - Protect /wp-admin/install.php (return 404/403).
  - Use a plugin to hide Server header or configure Apache to remove it.

2G. Add missing basic security headers `Security`

- **Impact:** Transport security, MIME sniffing
- **Problem:** Security basics verdict FAILED; HSTS and X-Content-Type-Options are missing despite HTTPS being active.
- **Solution:** Send from origin (Apache example):

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

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

2H. Fix list structure violations `Accessibility`

- **Impact:** Screen reader navigation, WCAG 1.3.1
- **Problem:** axe-core reports 2 serious violations where `<ul>` / `<ol>` contain non-`<li>` elements (e.g., links inside tags).
- **Solution:**
  - Ensure `<ul>` and `<ol>` only contain `<li>` elements directly.
  - Move links or tags inside the `<li>` wrapper, not as siblings.

2I. Fix color contrast and add main landmark `Accessibility`

- **Impact:** WCAG 1.4.3, 1.3.1, 2.4.1
- **Problem:** 1 serious violation on `.menu-item-75` contrast; missing `main` landmark and skip-to-content link.
- **Solution:**
  - Increase contrast ratio on `.menu-item-75` to ≥4.5:1.
  - Wrap main content in `<main>` tag.
  - Add `<a href="#main" class="skip-link">` before navigation.

2J. Correct HTML language and validation errors `SEO`

- **Impact:** Search indexing, Screen reader language detection
- **Problem:** HTML `lang="en"` on Estonian content; 10 W3C errors including invalid `script` attributes and `target` on `<p>`.
- **Solution:**
  - Change `<html lang="en">` to `<html lang="et">`.
  - Remove `target` attribute from `<p>` tags (use `<a>`).
  - Fix `script` tags: remove `async` / `src` from `type="text/plain"` data blocks.

Priority 3: Best Practice

Recommended for long-term maintainability.

3A. Fix W3C HTML validation errors `SEO`

- **Impact:** Parser recovery, SEO crawlability
- **Problem:** 16 errors including empty IDs (`id=""`), duplicate IDs, and invalid attributes on `<script>` and `<p>` tags.
- **Solution:**

- Remove empty `id` attributes or assign unique values.
- Ensure `<script type="text/plain">` does not use `src` or `async`.
- Remove `target` attribute from `<p>` elements.

3B. Add explicit width and height to images `Performance`

- **Impact:** CLS (Cumulative Layout Shift)
- **Problem:** 30 images lack width/height attributes, risking layout shifts despite current CLS of 0.089.
- **Solution:** Add `width` and `height` attributes to all `<img>` tags:

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

3C. Strengthen Content Security Policy (CSP) `Security`

- **Impact:** XSS Defense-in-Depth
- **Problem:** CSP is present but weak (missing `default-src`, `object-src`); site signals indicate no auth/payments, so this is lower priority.
- **Solution:** Update CSP header to include:

```
Content-Security-Policy: default-src 'self'; object-src 'none';
frame-ancestors 'self';
```

3D. Fix contrast and heading hierarchy `Accessibility`

- **Impact:** WCAG 1.4.3 contrast, 1.3.1 heading order
- **Problem:** axe-core found serious contrast issues on navigation links; W3C/axe noted h1→h3 skip.
- **Solution:**
  - Increase contrast ratio on `.navigation__link` to ≥4.5:1.
  - Change the first `h3` to `h2` to follow `h1` sequentially.

3E. Harden WordPress and refine CSP `Security`

- **Impact:** Brute-force protection, XSS defense-in-depth
- **Problem:** xmlrpc.php accepts POST (brute-force vector); CSP is weak (missing default-src/object-src). Site signals show no auth/payments, so CSP is P3.
- **Solution:**
  - Block POST to xmlrpc.php in .htaccess.
  - If adding user content later, implement strict CSP with nonce/hash.
  - Consider hiding /wp-login.php path.