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

Website: https://playandnope.com/
Date: 13.10.2026
Audit Coverage: 88% — W3C Validator: W3C HTTP 429
Confidence: medium

Pages Audited (1 of 1):

- https://playandnope.com/

Summary of results

Overall Score: 87 / 100
Status: □ □ **Needs Improvement**

PSI mobile 92 / desktop 96 with clean Core Web Vitals (LCP 2.4 s, CLS 0.001, TTFB 35 ms) makes performance a clear strength; only TBT (247 ms) and FCP (1.81 s) nudge past the 'good' thresholds, driven by jQuery and theme JS long tasks. Accessibility is near-perfect (PSI 100, 37 axe passes) but axe flags one serious color-contrast failure on `.menu-item-75 > .navigation__description`, and PSI's SEO audits fail on `link-text` (4 non-descriptive links, 'read more' ×4), `tapTargets` and `structuredData`. Security basics PASS, but the CSP is a stub (`frame-ancestors 'self'` only, no `default-src` / `object-src 'none'`), HSTS lacks `preload`, COOP/CORP are absent, and 2 jsdelivr scripts ship without SRI. Image handling is unusually clean (0 raster images, 0 missing alt, 0 missing lazy) though 5 images lack explicit dimensions and the document is served with `cache-control: max-age=0`. W3C validation could not run (HTTP 429), so HTML validity is unverified — this is the only coverage gap and it lowers confidence to medium.

Per-page scores

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

Score	Performance	Accessibility	Best Practices	SEO	Security
87	92	100	100	92	PASS

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	**92** / 96	**2.43 s** / 562 ms	0.001 / **0.099**

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. Fix color contrast on the navigation description `Accessibility`

- **Impact:** WCAG 1.4.3 (AA), axe serious violation
- **Problem:** axe-core reports 1 serious violation — `color-contrast` on `.menu-item-75 > .navigation__description` — and 8 further nodes where contrast could not be determined automatically.
- **Solution:**
  - Raise the text/background contrast ratio to at least **4.5:1** for normal text (3:1 for ≥18.66 px bold or ≥24 px).
  - Inspect the 8 'incomplete' nodes manually — axe skips elements with alpha transparency, gradients or background images.

```
.navigation__description { color: #4a4a4a; } /* verify against the actual nav background */
```

Priority 2: Important

Essential for compliance, user reach, and search visibility.

2A. Cut Total Blocking Time by breaking up long JS tasks `Performance`

- **Impact:** TBT, FCP, INP, Max Potential FID
- **Problem:** Mobile TBT is 247 ms (over the 200 ms 'good' threshold) and Max Potential FID is 150 ms; long tasks include `jquery.min.js` at 153 ms, `global.min.js` at 104 ms and `core.min.js` at 98/83/66 ms.
- **Solution:**
  - Drop jQuery if the theme allows — it is the single largest long task (153 ms).
  - Split `core.min.js` into route-level chunks so the main thread is not blocked by one 98 ms task.
  - In WP Rocket, enable **Delay JavaScript Execution** for non-critical scripts (cookie consent, iframe manager).
  - Audit the 22 scripts: 7 are deferred, 0 async — move analytics/consent to `async`.

2B. Stop serving the HTML document with cache-control: max-age=0 `Performance`

- **Impact:** Repeat-visit TTFB, LCP, FCP
- **Problem:** The document response sets `cache-control: max-age=0` with an `expires` timestamp already in the past, so browsers revalidate the HTML on every navigation despite WP Rocket being active.
- **Solution:** Serve the cached HTML with a short but non-zero lifetime plus stale-while-revalidate:

```
Cache-Control: public, max-age=600, stale-while-revalidate=86400
```

  Keep `max-age=0` only for logged-in or cart/checkout responses.

2C. Replace vague and repeated link text `Accessibility`

- **Impact:** PSI SEO `link-text`, WCAG 2.4.4, screen-reader navigation
- **Problem:** PSI's `link-text` audit fails with 4 links lacking descriptive text, and the inventory shows 'read more' repeated 4× plus 'design & innovation', 'development' and 'technical maintenance' each repeated 3×.
- **Solution:**
  - Rewrite 'read more' to name the destination, e.g. `<a href="/work/fintech">Read the Fintech case study</a>`.
  - Where the visible text must stay short, add an accessible name:

```
<a href="/services/development" aria-label="Development
services">Development</a>
```

2D. Add explicit width/height to the 5 unsized images `Performance`

- **Impact:** CLS (desktop 0.099 vs mobile 0.001)
- **Problem:** 5 of 30 images have no `width` / `height` attributes, and desktop CLS is 0.099 — roughly 100× the mobile value — with a recorded shift on `h1.hero__title`.
- **Solution:**
  - Add intrinsic `width` / `height` to every `<img>` so the browser can reserve space.
  - For fluid images, pair with CSS:

```
img { max-width: 100%; height: auto; }
```

  - Reserve space for the hero title block with `min-height` or `aspect-ratio` to absorb the recorded 0.001 shift.

2E. Complete HSTS and add COOP / CORP `Security`

- **Impact:** Transport security, origin isolation
- **Problem:** HSTS is `max-age=31536000; includeSubDomains` but lacks the `preload` directive, and both `Cross-Origin-Opener-Policy` and `Cross-Origin-Resource-Policy` are missing.
- **Solution:**

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

  Then submit the domain at hstspreload.org. Note: preload is effectively irreversible — confirm every subdomain is HTTPS-only first.

Priority 3: Best Practice

Recommended for long-term maintainability.

3A. Harden the Content-Security-Policy `Security`

- **Impact:** XSS defense-in-depth
- **Problem:** CSP is only `frame-ancestors 'self';` — no `default-src` and no `object-src 'none'`, so it restricts nothing beyond framing. Site signals show no auth, payments, user content or e-commerce, so XSS impact is limited and this is not a P1.
- **Solution:** If you later add a login or accept user content, deploy a nonce-based policy rather than a flat allowlist:

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

  At minimum add `default-src 'self'; object-src 'none';` today — it is a one-line change.

3B. Add Subresource Integrity to cross-origin scripts `Security`

- **Impact:** Supply-chain tampering risk
- **Problem:** 2 of 2 cross-origin scripts from `cdn.jsdelivr.net` (cookieconsent 3.0.1 and iframemanager 1.3.0) lack an `integrity` attribute, so a compromised CDN could inject arbitrary JS.
- **Solution:**

```
<script
src="https://cdn.jsdelivr.net/gh/orestbida/cookieconsent@3.0.1/dist
/cookieconsent.umd.js"
        integrity="sha384-…" crossorigin="anonymous" defer>
</script>
```

Generate the hash with `openssl dgst -sha384 -binary file.js | openssl base64 -A`. Better still, self-host both libraries.

3C. Add meaningful structured data `SEO`

- **Impact:** PSI `structuredData`, rich-result eligibility
- **Problem:** PSI's `structuredData` audit fails and the single JSON-LD block on the page is typed 'Unknown', so search engines get no machine-readable entity information.
- **Solution:** Emit a typed graph, e.g.:

```
{"@context":"https://schema.org","@type":"Organization","name":"Pla
y and Nope","url":"https://playandnope.com/","logo":"…","sameAs":
[…]}
```

Add `WebSite` with `potentialAction: SearchAction` and `Service` entries for the listed offerings.

3D. Enlarge mobile tap targets `Accessibility`

- **Impact:** PSI `tapTargets`, WCAG 2.5.8
- **Problem:** PSI's `tapTargets` audit fails on mobile, meaning some interactive elements are smaller than the 44×44 px minimum.
- **Solution:**
  - Give nav and footer links a minimum hit area:

```
a, button { min-height: 44px; min-width: 44px; display: inline-
flex; align-items: center; }
```

  - Add spacing between adjacent icon links so targets do not overlap.

3E. Trim legacy JavaScript and forced reflow `Performance`

- **Impact:** Bundle size, main-thread work
- **Problem:** PSI reports `legacy-javascript-insight` with an estimated 12 KiB saving and a `forced-reflow-insight` scoring 0.00, plus a `network-dependency-tree-insight` failure.
- **Solution:**

    - Add a modern browser target to the build (drop ES5 transpilation and core-js polyfills) to reclaim the 12 KiB.
    - Batch DOM reads before writes to eliminate forced synchronous layout.
    - Flatten the critical request chain: preload the LCP font/stylesheet and remove unnecessary serial dependencies.

3F. Reduce technology disclosure and move the login path `Security`

- **Impact:** Attack-surface enumeration
- **Problem:** The `Server: Apache` header discloses the web server, and the WordPress login form is served on the default `/wp-login.php` path — both flagged as warnings by the security checks.
- **Solution:**
    - Suppress the banner: `ServerTokens Prod` and `ServerSignature Off` in Apache config.
    - Move the login to a custom slug via a security plugin, and add rate limiting / 2FA on `/wp-login.php`.
    - Add `X-Permitted-Cross-Domain-Policies: none` while you are in the vhost.