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

Website: https://playandnope.com/
Date: 09.11.2026
Audit Coverage: 100% — all sources returned data
Confidence: medium

Pages Audited (5 of 5):

- https://playandnope.com/
- https://playandnope.com/privacy-policy/
- https://playandnope.com/digital-solutions-contact/
- https://playandnope.com/real-estate-digital-solutions/
- https://playandnope.com/industrial-digital-solutions/

Summary of results

Overall Score: 84 / 100
Status: **Needs Improvement**

What is pulling the score down

Points are for the weakest page; Pages = how many of 5 pages share the signal.

Signal	Points	Pages	Evidence
Performance 60	−16.0	5/5	weighted 40% of 40 points lost
Security basics	−10	5/5	FAILED: User enumeration blocked
HTML validation	−1	3/5	2 W3C errors
Best Practices 96	−0.6	1/5	weighted 15% of 4 points lost
Accessibility 99	−0.3	3/5	weighted 30% of 1 points lost
Advanced security headers	0	5/5	Failing: CSP is strict, Cross-Origin-Opener-Policy, Cross-Origin-Resource-Policy

Signal	Points	Pages	Evidence
Page score (weakest: https://playandnope.com/digital-solutions-contact/)	**72**		100 − 27.9 → 72

Site overall 84 is the mean of 5 pages; scores range 72 (https://playandnope.com/digital-solutions-contact/) → 88 (https://playandnope.com/privacy-policy/).

Per-page scores

 Needs Improvement · https://playandnope.com/

Base	Score	Performance	Accessibility	Best Practices	SEO	Security
97	87	96	100	100	92	FAILED

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

Base	Score	Performance	Accessibility	Best Practices	SEO	Security
98	88	96	100	100	100	FAILED

 Needs Improvement · https://playandnope.com/digital-solutions-contact/

Base	Score	Performance	Accessibility	Best Practices	SEO	Security
83	72	60	99	96	100	FAILED

 Needs Improvement · https://playandnope.com/real-estate-digital-solutions/

Base	Score	Performance	Accessibility	Best Practices	SEO	Security
97	86	93	98	100	100	FAILED

 Needs Improvement · https://playandnope.com/industrial-digital-solutions/

Base	Score	Performance	Accessibility	Best Practices	SEO	Security
98	87	97	98	100	100	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/	**96** / 97	**1.66 s** / 448 ms	0.000 / **0.084**
https://playandnope.com/privacy-policy/	**96** / 98	**2.55 s** / 445 ms	0.000 / **0.084**
https://playandnope.com/digital-solutions-contact/	**60** / 75	**8.25 s** / 486 ms	0.000 / **0.083**
https://playandnope.com/real-estate-digital-solutions/	**93** / 98	**2.86 s** / 491 ms	0.000 / **0.083**
https://playandnope.com/industrial-digital-solutions/	**97** / 98	**1.96 s** / 485 ms	0.000 / **0.083**

Optimization Checklist

2 of 3 passing — 2 pass · 1 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 br.
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.

Item	Status	Detail
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	**Warn**	2 render-blocking scripts in . Move to footer or add defer/async.

Fixes

Priority 1: Critical

Immediate action — impacts user experience, search rankings, or site safety.

1A. Block WordPress user enumeration `Security`

- **Impact:** Security basics row (−10), Security basics verdict, username harvesting for brute-force attacks
- **Problem:** The Security basics verdict is FAILED solely because "WordPress usernames can be enumerated" — author archives and the REST users endpoint expose login names, which feeds credential-stuffing attacks against /wp-login.php.
- **Solution:**
  - Disable the REST users endpoint for anonymous visitors and block `?author=N` scans:

```
add_filter('rest_endpoints', function($e){
  if(!is_user_logged_in()){ unset($e['/wp/v2/users'],
$e['/wp/v2/users/(?P<id>[\d]+)']); }
  return $e;
});
add_action('template_redirect', function(){
  if(is_author() && !is_user_logged_in()){
wp_safe_redirect(home_url(), 301); exit; }
});
```

  - Ensure author slugs differ from login names, and add rate limiting / 2FA on the login form.

1B. Defer or lazy-load reCAPTCHA to fix mobile LCP `Performance`

- **Impact:** LCP, TBT, TTI, Speed Index

- **Problem:** Mobile LCP is 8.3 s (desktop 0.5 s) and TTI 12.9 s; recaptcha__en.js alone is 351 KB / 921 ms and appears in 8 long tasks totalling ~1 s, with 177 KB reported as unused JS.
- **Solution:**
  - Load reCAPTCHA only when the contact form is focused or submitted instead of on page load:

```
form.addEventListener('focusin', () => loadRecaptcha(), { once:
true });
```

  - If the plugin supports it, switch to reCAPTCHA v3 with `render=explicit` and a deferred load, or replace it with a honeypot/rate-limit check.
  - Re-measure mobile LCP after the change; the 8.3 s → sub-2.5 s gap is almost entirely third-party script cost.

1C. Fix W3C validation errors `Best Practices`

- **Impact:** HTML validation row (−1), HTML validity, form semantics
- **Problem:** The W3C validator reports 2 errors: a hidden input carrying `autocomplete='off'` (first at line 885, `gform_hidden`).
- **Solution:** Remove `autocomplete` from hidden Gravity Forms inputs, or set it via a filter so it is not rendered on `type="hidden"` fields:

```
<input type="hidden" class="gform_hidden"
name="gform_target_page_number_1" value="0">
```

Priority 2: Important

Essential for compliance, user reach, and search visibility.

2A. Remove render-blocking and unused CSS `Performance`

- **Impact:** Speed Index, FCP, render-blocking chain
- **Problem:** Mobile Speed Index is 4.49 s (score 0.72) with an estimated 670 ms of render-blocking savings, plus 11 KiB of legacy JavaScript; the network dependency tree is flagged as a high-severity insight.
- **Solution:**
  - Inline the critical CSS for the hero/above-the-fold section and load the 3 external stylesheets asynchronously (`media="print" onload="this.media='all'"` or `rel="preload"` + swap).
  - Defer the cookie-consent / iframemanager bundles from cdn.jsdelivr.net until interaction.

- Drop the jQuery + jQuery-migrate pair if the theme scripts no longer need it (30.7 KB + migrate).
- Replace legacy polyfills flagged by `legacy-javascript-insight` with modern syntax targets.

2B. Make link text descriptive `SEO`

- **Impact:** SEO (link-text audit), screen-reader link lists
- **Problem:** The `link-text` audit fails with 4 links lacking descriptive text, and the HTML inventory shows "read more" repeated 4 times plus service names repeated 3 times each.
- **Solution:**
  - Replace each "read more" with the destination, e.g. `<a href="/work/fintech">Read the fintech case study</a>`.
  - Where the visible text must stay short, disambiguate with `aria-label` or a visually hidden span:

```
<a href="/work/fintech">Read more<span class="sr-only"> about the
fintech case study</span></a>
```

2C. 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 else.
- **Solution:** Add a nonce-based policy rather than a flat allowlist:

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

  Note the page loads reCAPTCHA from gstatic/google and cookie-consent from jsDelivr — allow those origins explicitly while migrating.

2D. Add Subresource Integrity to third-party scripts `Security`

- **Impact:** Supply-chain tampering risk
- **Problem:** 3 of 4 cross-origin scripts lack an `integrity` attribute (jsDelivr iframemanager, cookieconsent, and others).
- **Solution:** Pin versions and add hashes:

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

Self-host the two jsDelivr bundles if hashes cannot be maintained.

2E. Protect the WordPress login and installer `Security`

- **Impact:** Brute-force and credential-stuffing surface
- **Problem:** The login form is served on the default `/wp-login.php` path (flagged as a warning), which is the first target for automated attack traffic.
- **Solution:**
  - Move or mask the login URL (e.g. WPS Hide Login) or restrict `/wp-login.php` by IP at the server.
  - Add rate limiting and 2FA on the login form.
  - Keep `xmlrpc.php` blocked (already passing) and confirm the installer paths stay unreachable.

2F. Verify color contrast manually `Accessibility`

- **Impact:** WCAG 1.4.3 contrast, readability of navigation descriptions
- **Problem:** axe-core reports one serious `color-contrast` violation on `.menu-item-74 > .navigation__description` and `.menu-item-75 > .navigation__description`, with 2 further nodes it could not determine.
- **Solution:**
  - Measure the description text against its background and raise it to at least 4.5:1 (3:1 for large text).
  - Check the 2 "incomplete" nodes manually, since axe skips gradients and alpha-transparent backgrounds.
  - Re-run axe after the CSS change to confirm the violation clears.

2G. Remove render-blocking scripts from the document head `Performance`

- **Impact:** FCP, LCP, Speed Index
- **Problem:** 11 external scripts are render-blocking (only 7 defer, 1 async); the checklist flags iframemanager.js and cookieconsent.umd.js loading synchronously in `<head>`.
- **Solution:**
  - Add `defer` to the cookie-consent and iframe-manager bundles:

```
<script
src="https://cdn.jsdelivr.net/gh/orestbida/cookieconsent@3.0.1/dist
/cookieconsent.umd.js" defer></script>
```

- Move non-critical theme scripts to the footer and audit the remaining 11 blocking tags for defer/async.

2H. Add Referrer-Policy, Permissions-Policy, COOP and CORP `Security`

- **Impact:** Cross-origin isolation, referrer leakage
- **Problem:** Cross-Origin-Opener-Policy and Cross-Origin-Resource-Policy are both missing (Referrer-Policy and Permissions-Policy are already set correctly).
- **Solution:**

```
Header always set Cross-Origin-Opener-Policy "same-origin"
Header always set Cross-Origin-Resource-Policy "same-site"
```

Verify embedded reCAPTCHA iframes and jsDelivr assets still load after enabling COOP.

2I. Label the unlabeled form field `Accessibility`

- **Impact:** Form accessibility, WCAG 1.3.1 / 4.1.2
- **Problem:** The contact form's textarea has no associated label (axe reports 1 minor violation and 3 undetermined contrast nodes).
- **Solution:**
  - Add a visible `<label for="…">` or `aria-label` to the textarea.
  - Manually verify contrast on the 3 nodes axe could not evaluate.

2J. Fix heading hierarchy `Accessibility`

- **Impact:** Screen-reader navigation, WCAG 1.3.1 / heading-order
- **Problem:** axe-core flags `heading-order` (moderate) on `.hero__description > h3`, and the W3C validator reports the same h1 → h3 skip; the outline has h1 ×1, h2 ×4, h3 ×13 with no h4.
- **Solution:**
  - Promote the hero `<h3>` to `<h2>`.
  - Audit the remaining h3s (Results, Index, Get in touch) and insert h2 section headings where a level is skipped.
  - Keep one h1 per page and never skip levels downward.

Priority 3: Best Practice

Recommended for long-term maintainability.

3A. Add COOP and CORP headers `Security`

- **Impact:** Cross-origin isolation, cross-window attacks
- **Problem:** Cross-Origin-Opener-Policy and Cross-Origin-Resource-Policy are both missing from the response, while Referrer-Policy and Permissions-Policy are already correctly set.
- **Solution:**

  ```
  Header always set Cross-Origin-Opener-Policy "same-origin"
  Header always set Cross-Origin-Resource-Policy "same-origin"
  Header always set X-Permitted-Cross-Domain-Policies "none"
  ```

  Verify embedded third-party frames (cookie-consent iframes) still work after enabling COOP.

3B. Enable HSTS preload `Security`

- **Impact:** First-visit downgrade protection
- **Problem:** HSTS is set to `max-age=31536000; includeSubDomains` but lacks the `preload` directive, so the very first request can still be downgraded.
- **Solution:**
  - Append `preload` to the header: `Strict-Transport-Security: max-age=31536000; includeSubDomains; preload`.
  - Confirm every subdomain is HTTPS-only, then submit the domain at hstspreload.org.

3C. Hide server version headers `Security`

- **Impact:** Technology disclosure
- **Problem:** The response advertises `Server: Apache`, which the Security basics checklist flags as a technology-disclosure warning.
- **Solution:**

  ```
  ServerTokens Prod
  ServerSignature Off
  ```

  Also strip any `X-Powered-By` header emitted by PHP.

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

- **Impact:** CLS

- **Problem:** 5 of 30 images have no width/height attributes; desktop CLS is 0.084 and the inventory flags missing dimensions as a layout-shift risk.
- **Solution:**
  - Add intrinsic `width` / `height` (or `aspect-ratio` in CSS) to the 5 images lacking them, including the SVG placeholders.
  - Keep `loading="lazy"` on below-the-fold media and reserve space for the lazy placeholders.

3E. Enlarge touch targets `Accessibility`

- **Impact:** Mobile tap accuracy (WCAG 2.5.8)
- **Problem:** The PSI `tapTargets` audit fails on mobile, and axe cannot verify target size automatically.
- **Solution:**
  - Ensure every nav link, icon button and footer link is at least 44×44 px with adequate spacing.

```
.nav a, .icon-btn { min-width: 44px; min-height: 44px; display:
inline-flex; align-items: center; justify-content: center; }
```

3F. Add structured data `SEO`

- **Impact:** Rich results eligibility
- **Problem:** The PSI `structuredData` audit fails and the single JSON-LD block is reported with type "Unknown", so search engines get no usable entity markup.
- **Solution:**
  - Emit valid `Organization` and `WebSite` JSON-LD with name, url, logo and sameAs.
  - Add `Service` items for the listed offerings if they have dedicated pages.
  - Validate with the Rich Results Test after deployment.

3G. Add Cross-Origin-Opener-Policy and Cross-Origin-Resource-Policy `Security`

- **Impact:** Cross-origin isolation, cross-origin read protection
- **Problem:** Both COOP and CORP are missing from the response headers (advanced checks fail; the site has no auth, payments or user content, so risk is low).
- **Solution:**

```
Header always set Cross-Origin-Opener-Policy "same-origin"
Header always set Cross-Origin-Resource-Policy "same-site"
```

    - Verify embedded third-party content (jsdelivr scripts, iframes) still loads after enabling CORP.

3H. Add a meta description `SEO`

- **Impact:** Search snippet quality
- **Problem:** The meta description is the WordPress placeholder "Our website address is: https://playandnope.com." rather than a description of the page.
- **Solution:**
    - Write a 120–155 character summary of the privacy policy (what data is collected, cookies, contact).
    - Replace the auto-generated description in the SEO plugin / theme settings.

3I. Fix console errors from reCAPTCHA `Best Practices`

- **Impact:** Best Practices (errors-in-console)
- **Problem:** 5 console events: `requestStorageAccess: Permission denied` (×2), a CORS-blocked `styles__ltr.css` request and `net::ERR_FAILED`.
- **Solution:**
    - These originate inside the reCAPTCHA iframe; removing or lazy-loading reCAPTCHA (see the LCP fix) eliminates them.
    - If reCAPTCHA stays, ensure the badge/iframe is not blocked by cookie-consent or COOP settings.

3J. Cache the HTML document `Performance`

- **Impact:** Repeat-visit TTFB
- **Problem:** The document is served with `cache-control: max-age=0` and PSI's cache insight estimates ~1 KiB of savings.
- **Solution:** Allow short-lived shared caching for anonymous visitors via WP Rocket / the CDN, e.g. `Cache-Control: public, max-age=600, s-maxage=3600`.

3K. Reduce unused and legacy JavaScript `Performance`

- **Impact:** TBT, main-thread work, mobile LCP
- **Problem:** PSI reports 30 KB of unused JavaScript on this URL and the `legacy-javascript-insight` estimates 11 KiB of savings; 8 scripts totalling 100.3 KB are loaded, including jQuery and jquery-migrate.
- **Solution:**

- Drop `jquery-migrate.min.js` if no legacy plugin depends on it.
- Ship modern syntax only (remove Babel/polyfill output for evergreen browsers).
- Defer or conditionally load scripts used only by below-the-fold components.