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 (5 of 5):

- https://playandnope.com/
- https://playandnope.com/privacy-policy
- https://playandnope.com/contact
- https://playandnope.com/full-stack-digital-agency
- https://playandnope.com/digital-solutions-contact

Summary of results

Overall Score: 79 / 100
Status: □ □ **Needs Improvement**

Site overall 79 is the mean of 5 pages. Scores range 58 (https://playandnope.com/digital-solutions-contact) → 89 (https://playandnope.com/full-stack-digital-agency). Weakest page: Performance is the dominant drag: PSI mobile 54 / desktop 58, with mobile LCP 6.5 s (heavy penalty), TBT 865 ms, TTI 11.7 s, and FCP 1.98 s — desktop is materially better on LCP (1.8 s) but worse on CLS (0.256 vs 0.070). The root cause is third-party reCAPTCHA: 1.44 MB from gstatic across 10 requests, three 172–173 KB unused-JS entries, and 10 long tasks up to 309 ms. Accessibility (99) and SEO (100) are excellent — axe reports only 1 minor violation — and the Security basics verdict is PASS, though advanced checks fail (CSP lacks default-src/object-src, HSTS lacks preload, COOP/CORP missing). Image assets are a non-issue (5 SVGs, no raster images). The W3C validator returned HTTP 429, so HTML validity is unscored; confidence is medium.

Per-page scores

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

Score	Performance	Accessibility	Best Practices	SEO	Security
85	96	100	100	92	PASS

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

Score	Performance	Accessibility	Best Practices	SEO	Security
88	91	100	100	100	PASS

 Needs Improvement · https://playandnope.com/contact

Score	Performance	Accessibility	Best Practices	SEO	Security
75	74	99	96	100	PASS

 Needs Improvement · https://playandnope.com/full-stack-digital-agency

Score	Performance	Accessibility	Best Practices	SEO	Security
89	95	98	100	100	PASS

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

Score	Performance	Accessibility	Best Practices	SEO	Security
58	54	99	96	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/	96 / **82**	**2.58 s** / 621 ms	0.014 / **0.366**
https://playandnope.com/privacy-policy	**91** / 97	**3.00 s** / 580 ms	0.090 / **0.101**
https://playandnope.com/contact	**74** / 88	**6.07 s** / 663 ms	0.000 / **0.083**

URL	Performance (M / D)	LCP (M / D)	CLS (M / D)
https://playandnope.com/full-stack-digital-agency	**95** / 98	**2.59 s** / 618 ms	0.010 / **0.084**
https://playandnope.com/digital-solutions-contact	**54** / 58	**6.52 s** / 1.77 s	0.070 / **0.256**

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. Eliminate the desktop layout shift (CLS 0.366) `Performance`

- **Impact:** CLS, desktop UX, PSI desktop performance
- **Problem:** Desktop CLS is 0.366 (heavy-penalty band) versus 0.014 on mobile; the mobile shift source is `div.hero__inner > div.grid > div.grid__col > h1.hero__title`, and 5 images lack explicit width/height.
- **Solution:**
  - Reserve space for the hero title and any late-loading content with `min-height` / `aspect-ratio` on the container.
  - Add explicit `width` / `height` (or `aspect-ratio`) to the 5 images missing dimensions.
  - Preload the hero font and any above-the-fold image so the swap does not reflow text.
  - Re-run PSI desktop after each change; target CLS ≤ 0.1.

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

- **Impact:** WCAG 1.4.3 (AA), axe serious violation
- **Problem:** axe reports 1 serious `color-contrast` violation on `.menu-item-74 > .navigation__description` and `.menu-item-75 > .navigation__description`, with 8 further nodes axe could not determine.
- **Solution:**
  - Darken the `.navigation__description` text color to reach ≥4.5:1 against its background (or lighten the background).
  - Manually verify the 8 undetermined nodes (alpha/gradient backgrounds) with a contrast checker.
  - Also check the `link-in-text-block` incomplete node — links must be distinguishable without relying on color alone (add underline or a non-color cue).

1C. Fix color-contrast on navigation description text `Accessibility`

- **Impact:** WCAG 1.4.3, axe serious violation
- **Problem:** axe reports 1 serious violation: `.menu-item-75 > .navigation__description` fails minimum color contrast (WCAG 2 AA).

- **Solution:** Raise the foreground/background contrast ratio to ≥4.5:1 for normal text (≥3:1 for large text).

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

  Re-run axe after the change; 9 additional nodes were flagged as "incomplete" (alpha/gradient backgrounds) and should be checked manually.

1D. Load reCAPTCHA lazily instead of on page load `Performance`

- **Impact:** LCP, TBT, TTI, Speed Index, page weight
- **Problem:** recaptcha__en.js accounts for 176/170/169 KB of unused JS, six long tasks of 55–101 ms, and 1.44 MB of the 1.91 MB total page weight; mobile LCP is 6.1 s vs 0.7 s on desktop.
- **Solution:**
  - Render the reCAPTCHA widget only when the user focuses or submits the form (explicit render on interaction), not on initial load.
  - If using Gravity Forms, enable the reCAPTCHA v3 "defer" / lazy-load option, or switch to a lighter challenge (e.g. Turnstile) that ships a smaller bundle.
  - Preconnect to `https://www.gstatic.com` only if the widget is still loaded eagerly.

1E. Strengthen the Content-Security-Policy `Security`

- **Impact:** XSS defense-in-depth
- **Problem:** CSP is `frame-ancestors 'self';` only — no `default-src`, no `object-src 'none'`, and no script/resource restrictions. The contact form includes a `<textarea>` (user-content signal), so a real XSS surface exists.
- **Solution:** Deploy a nonce-based CSP with `'strict-dynamic'` 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';
    form-action 'self';
  ```

  - Add the nonce to every `<script>` tag emitted by WordPress/Gravity Forms.
  - Roll out in `Content-Security-Policy-Report-Only` first to catch breakage.

1F. Fix color-contrast failure on the navigation description `Accessibility`

- **Impact:** WCAG 1.4.3 (wcag2aa), axe serious violation
- **Problem:** axe reports a serious color-contrast violation on `.menu-item-75 > .navigation__description`, and 9 further nodes were flagged 'incomplete' because axe could not resolve contrast (alpha/gradient backgrounds).
- **Solution:**
  - Raise the nav description text to at least **4.5:1** against its background (3:1 if ≥18.66 px bold / ≥24 px).
  - Manually verify the 9 'incomplete' nodes — axe skips elements with alpha transparency or gradients, so check them with a contrast picker.
  - Example: if the description sits on `#1a1a1a`, use `#8a8a8a` or lighter; if on white, use `#595959` or darker.

1G. Defer / lazy-init reCAPTCHA to cut third-party blocking cost `Performance`

- **Impact:** TBT, TTI, LCP, page weight
- **Problem:** reCAPTCHA from www.gstatic.com accounts for 1.44 MB across 10 requests, three 172–173 KB unused-JS entries, and 10 long tasks (309 ms, 277 ms, 261 ms, 233 ms, …). Mobile TBT is 865 ms and TTI 11.7 s.
- **Solution:** Load reCAPTCHA only when the user focuses the form, and use explicit render:

```
<script src="https://www.google.com/recaptcha/api.js?
render=explicit&hl=en" defer></script>
<script>
  document.querySelector('form textarea').addEventListener('focus',
() => {
    grecaptcha.ready(() => grecaptcha.execute('SITE_KEY', {action:
'contact'}));
  }, {once: true});
</script>
```

  - If the challenge is not strictly required, evaluate Cloudflare Turnstile (lighter payload).
  - Keep the script off the critical path so it does not compete with LCP.

1H. Fix mobile LCP (6.5 s) and render-blocking scripts `Performance`

- **Impact:** LCP, FCP, Speed Index
- **Problem:** Mobile LCP is 6.5 s vs 1.8 s on desktop; PSI flags `document-latency-insight` (est. 540 ms savings) and 2 render-blocking scripts remain in the document.
- **Solution:**

- Identify the LCP element in DevTools Performance panel and preload it:

```
<link rel="preload" as="image" href="/path/to/hero.webp"
fetchpriority="high">
```

- Add `defer` (or `async`) to the 2 render-blocking scripts; inline critical CSS for above-the-fold content.
- Reduce document latency — the HTML is 134 KB and the document request took 508 ms.

Priority 2: Important

Essential for compliance, user reach, and search visibility.

2A. Replace vague repeated link text `SEO`

- **Impact:** SEO `link-text` audit, screen-reader link lists
- **Problem:** The SEO `link-text` audit fails with 4 links lacking descriptive text, and the inventory shows "read more" repeated ×4 plus repeated nav labels ("business transformation" ×3, "development" ×3, etc.).
- **Solution:**
  - Give each "read more" link a unique, descriptive label, e.g. `<a href="/case-study-x">Read the Fintech case study</a>`.
  - Where the visible text must stay short, disambiguate with `aria-label` or visually-hidden text:

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

2B. Increase touch target sizes `Accessibility`

- **Impact:** SEO `tapTargets` audit, WCAG 2.5.8
- **Problem:** PSI reports the `tapTargets` audit failing, and the manual-check list flags the 44×44 px minimum as unverified.
- **Solution:**
  - Ensure every interactive element (nav links, icon buttons, footer links) has a hit area of at least 44×44 px.
  - Use padding rather than enlarging the icon:

```
.navigation__link { display:inline-flex; align-items:center; min-
height:44px; min-width:44px; padding:10px 12px; }
```

2C. Resolve forced reflow and the deep network dependency chain `Performance`

- **Impact:** TBT, INP, main-thread work
- **Problem:** PSI flags `forced-reflow-insight` **(high)** and `network-dependency-tree-insight` **(high)**; two theme scripts (`core.*.min.js` 61 ms, `jquery.*.min.js` 57 ms) are the longest tasks.
- **Solution:**
  - Batch DOM reads before writes; avoid reading `offsetHeight` / `getBoundingClientRect()` inside loops or after style mutations.
  - Break the critical request chain: preload the fonts and the first stylesheet, and inline critical CSS.
  - Defer non-critical theme JS and audit whether jQuery + jQuery Migrate are still required.

2D. Add valid structured data `SEO`

- **Impact:** SEO `structuredData` audit, rich results eligibility
- **Problem:** The `structuredData` audit fails and the single JSON-LD block is typed as `Unknown` , so search engines get no usable entity markup.
- **Solution:**
  - Emit a valid `Organization` (or `ProfessionalService`) JSON-LD block with `name` , `url` , `logo` , `sameAs` , and `contactPoint` .
  - Validate with the Rich Results Test and Schema Markup Validator after deploy.

2E. Fix document cache policy (cache-control: max-age=0) `Performance`

- **Impact:** Repeat-visit TTFB, LCP
- **Problem:** The document response sends `cache-control: max-age=0` with an `expires` equal to the request time, forcing revalidation on every navigation despite WP Rocket being active.
- **Solution:**
  - Set a short but non-zero browser TTL for HTML and rely on `stale-while-revalidate` :

```
Cache-Control: public, max-age=60, stale-while-revalidate=300
```

  - Keep long-lived immutable caching for hashed theme assets (`/wp-content/themes/.../js/*.min.js`).

2F. Reduce mobile LCP (3.0 s) and FCP (2.0 s) `Performance`

- **Impact:** LCP, FCP, Speed Index
- **Problem:** Mobile LCP is 3.0 s vs 0.6 s desktop and FCP 2.0 s vs 540 ms; PSI flags `document-latency-insight` (est. 550 ms savings), `forced-reflow-insight`, and `legacy-javascript-insight` (12 KiB).
- **Solution:**
  - Eliminate the forced reflow: batch DOM reads/writes in `core.*.min.js` and `global.*.min.js` (the two long tasks at 67 ms and 52 ms).
  - Drop legacy JS transpilation targets so modern browsers skip the 12 KiB polyfill bundle.
  - Preload the LCP element and any critical font; add `fetchpriority="high"` to the hero asset.
  - Reduce the network dependency chain flagged by `network-dependency-tree-insight`.

2G. Eliminate cookie-consent banner layout shift `Performance`

- **Impact:** CLS (0.089 mobile / 0.101 desktop)
- **Problem:** The dominant layout-shift source is `body.privacy-policy > div#cc-main > div.cm-wrapper > div.cm` (shift 0.089), pushing desktop CLS to 0.101 — just over the 0.1 threshold.
- **Solution:** Reserve space for the consent banner before it renders:

  ```
  #cc-main .cm-wrapper { position: fixed; inset: auto 0 0 0; min-height: 96px; }
  ```

  Or render the banner server-side / with `content-visibility` so it does not reflow the document on hydration.

2H. Serve the document with a positive cache lifetime `Performance`

- **Impact:** Repeat-visit TTFB, cache hit rate
- **Problem:** The document response returns `cache-control: max-age=0` with an `expires` in the past, despite WP Rocket being detected — every visit revalidates.
- **Solution:** Configure WP Rocket (or the origin) to emit a real cache lifetime for anonymous HTML:

  ```
  Cache-Control: public, max-age=600, s-maxage=86400, stale-while-revalidate=60
  ```

  Ensure logged-in / cart / preview requests bypass the cache.

2I. Enlarge tap targets `Accessibility`

- **Impact:** WCAG 2.5.8, PSI `tapTargets` audit
- **Problem:** PSI's `tapTargets` audit fails on mobile — interactive elements are smaller than the 44×44 px minimum.
- **Solution:**
  - Add padding to nav links and icon buttons so the hit area is ≥44×44 px.
  - Use `min-height: 44px; min-width: 44px;` on `.navigation__link` and any icon-only controls.
  - Verify with Chrome DevTools' "Emulate touch" + the Lighthouse tap-targets audit.

2J. Add Subresource Integrity to cross-origin scripts `Security`

- **Impact:** Supply-chain integrity for jsdelivr assets
- **Problem:** 2 of 2 cross-origin scripts (iframemanager.js, cookieconsent.umd.js from cdn.jsdelivr.net) lack an `integrity` attribute.
- **Solution:** Pin the exact version and add SRI hashes:

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

  Generate hashes with `openssl dgst -sha384 -binary file.js | openssl base64 -A`.

2K. Fix document latency and the /contact redirect `Performance`

- **Impact:** LCP, FCP, TTFB
- **Problem:** PSI flags `document-latency-insight` as high priority with an estimated 650 ms savings, and the slowest request is the `/contact` document at 479 ms returning 0 B while the final URL is `/digital-solutions-contact/`.
- **Solution:**
  - Serve the canonical URL directly so `/contact` does not incur a redirect hop.
  - Ensure the HTML document is served from cache (WP Rocket) rather than regenerated per request.
  - Verify the redirect chain in DevTools Network panel and collapse any multi-hop redirects into a single 301.

2L. Resolve reCAPTCHA console errors and failed request `Best Practices`

- **Impact:** Console errors, Best Practices score

- **Problem:** 5 console events including two `requestStorageAccess: Permission denied`, a CORS block on `styles__ltr.css` from gstatic, and a `net::ERR_FAILED` on the same stylesheet; PSI's `errors-in-console` audit fails.
- **Solution:**
  - Ensure the cookie-consent / iframe-manager configuration does not block storage access for the reCAPTCHA iframe.
  - Confirm the reCAPTCHA site key and domain allowlist in the Google reCAPTCHA admin console include `playandnope.com`.
  - Re-test after the lazy-load change above; the CORS failure is often a symptom of the widget loading before consent state is resolved.

2M. Label the unlabeled textarea in the contact form `Accessibility`

- **Impact:** WCAG 1.3.1, 4.1.2, form usability
- **Problem:** Form 1 contains a `textarea` with no associated label (the text inputs are labeled, the textarea is not).
- **Solution:**

```
<label for="message">Your message</label>
<textarea id="message" name="message" rows="6"></textarea>
```

  - If a visible label is not desired, use `aria-label="Your message"` instead.

2N. Add HSTS preload directive `Security`

- **Impact:** Transport security
- **Problem:** HSTS is `max-age=31536000; includeSubDomains` but lacks `preload`, flagged as a high-priority weakness.
- **Solution:**

```
Strict-Transport-Security: max-age=63072000; includeSubDomains;
preload
```

  - Then submit the domain at https://hstspreload.org/ and confirm all subdomains are HTTPS-only.

2O. Fix heading-order skip (h1 → h3) `Accessibility`

- **Impact:** WCAG 1.3.1, PSI heading-order audit (score 0.00)
- **Problem:** PSI's `heading-order` audit scores 0.00 and axe flags `.hero__description > h3`; the document outline jumps from h1 "Get to know us" straight to h3 "Full-stack digital agency powered by curiosity".
- **Solution:**

    - Change the hero `<h3>` to `<h2>` so the outline descends one level at a time.
    - Audit the remaining h3s (12 total, 0 h4–h6) and promote any that are top-level sections to h2.
    - Keep h1 unique per page.

2P. Harden the Content-Security-Policy `Security`

- **Impact:** XSS defense-in-depth, CSP strictness check
- **Problem:** CSP is `frame-ancestors 'self';` only — no `default-src` and no `object-src 'none'`, so script and resource loading are entirely unrestricted. The site serves a WordPress login at `/wp-login.php`, so an XSS foothold would be valuable.
- **Solution:** Add a nonce-based policy rather than a flat allowlist:

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

    - Emit the nonce per request from WordPress and tag every `<script>` with it.
    - Roll out in `Content-Security-Policy-Report-Only` first and watch for violations.

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

- **Impact:** Repeat-visit TTFB, LCP, document latency
- **Problem:** The document response is `cache-control: max-age=0` with `expires` set to the request time, so browsers revalidate the 195 KB HTML on every navigation even though WP Rocket is active.
- **Solution:**
    - Serve a short browser TTL with revalidation for HTML:

```
Cache-Control: public, max-age=60, stale-while-revalidate=300
```

    - Keep the long TTL on hashed static assets (`/wp-content/...`) — those are immutable.
    - If a CDN fronts the site, let it cache HTML at the edge and purge on publish.

2R. Eliminate forced reflow and reduce document latency `Performance`

- **Impact:** TBT, INP, LCP, FCP
- **Problem:** PSI flags `forced-reflow-insight` **(high)** and `document-latency-insight` (high, est. 530 ms savings); the runtime capture shows the document request taking 491 ms and jQuery producing a 60 ms long task.
- **Solution:**
  - Batch DOM reads before writes; avoid interleaving `offsetHeight` / `getBoundingClientRect` with style mutations in the theme JS.
  - Defer or lazy-init jQuery-dependent widgets below the fold.
  - Investigate the 491 ms document response — check WP Rocket cache warm-up and any server-side plugin work on this URL.

2S. Move the WordPress login off the default /wp-login.php path `Security`

- **Impact:** Brute-force / credential-stuffing surface
- **Problem:** Security basics flags 'Login not on default path — warn': the login form is served on the default `/wp-login.php` path, which is the first URL automated credential-stuffing tools try.
- **Solution:**
  - Rename the login URL (e.g. WPS Hide Login or a server-level rewrite) and return 404 on `/wp-login.php`.
  - Add rate limiting and 2FA on the login endpoint.
  - Keep `xmlrpc.php` blocked (already passing).

2T. Eliminate desktop layout shift (CLS 0.256) `Performance`

- **Impact:** CLS
- **Problem:** Desktop CLS is 0.256 — above the 0.25 'poor' threshold — with a 0.070 shift attributed to `body.wp-singular > div#page > main#main-content > div.section`.
- **Solution:**
  - Reserve space for the shifting section with explicit `min-height` or `aspect-ratio`.
  - Set `width` / `height` on any injected media (ads, embeds, cookie banner).
  - Avoid inserting content above existing content after first paint; use `transform` animations instead of layout-affecting properties.

2U. Resolve console errors and the failed reCAPTCHA stylesheet `Best Practices`

- **Impact:** Best Practices score, form reliability
- **Problem:** 5 console events were captured, including two `requestStorageAccess: Permission denied.` errors and a CORS-blocked `styles__ltr.css` (`net::ERR_FAILED`); PSI's `errors-in-console` audit fails.
- **Solution:**
  - The CORS failure on `https://www.gstatic.com/recaptcha/releases/.../styles__ltr.css` originates from the reCAPTCHA iframe — verify the site key is registered for `playandnope.com` in the reCAPTCHA admin console.
  - The `requestStorageAccess` denials come from the cookie-consent / iframe-manager stack; check that the consent script does not block storage access before reCAPTCHA initializes.
  - Re-run the audit after fixing to confirm `errors-in-console` passes.

2V. Label the unlabeled textarea and verify contrast `Accessibility`

- **Impact:** WCAG 1.3.1, 1.4.3, 2.4.4
- **Problem:** Form 1 contains a `<textarea>` with no label (plus 12 unlabeled hidden inputs); axe also left 10 color-contrast nodes and 1 link-in-text-block node as 'incomplete'.
- **Solution:**
  - Add a visible `<label for="...">` or `aria-label` to the unlabeled textarea:

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

  - Manually verify the 10 color-contrast nodes axe could not resolve (alpha/gradient backgrounds).
  - Ensure in-text links are distinguishable by more than color (underline on hover/focus).

2W. Disambiguate repeated link text `SEO`

- **Impact:** Link purpose (WCAG 2.4.4), crawl clarity
- **Problem:** 10 link texts repeat across the page — e.g. "info@playandnope.com" ×3, "home" ×2, "work" ×2, "about" ×2, "contact" ×2 — and PSI's `tapTargets` and `structuredData` modeled audits fail.
- **Solution:**
  - Add `aria-label` to repeated links to distinguish destination:

```
<a href="/work" aria-label="View our work portfolio">work</a>
```

- Expand the JSON-LD block (currently typed as `Unknown`) to a recognized schema such as `Organization` or `ContactPage`.
- Increase tap-target sizes to at least 44×44 px.

Priority 3: Best Practice

Recommended for long-term maintainability.

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

- **Impact:** XSS defense-in-depth
- **Problem:** CSP is present but weak — only `frame-ancestors 'self'` is set, with `default-src` missing and `object-src` not `'none'`. Site signals show no auth, payments, or user content, so this is defense-in-depth rather than an active exposure.
- **Solution:**
  - Add the missing directives at minimum:

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

  - If you later add login or user content, move to a nonce + `'strict-dynamic'` script policy rather than a flat allowlist.

3B. Add HSTS preload, COOP and CORP `Security`

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

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

  Submit the domain at hstspreload.org once the preload directive is live.

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

- **Impact:** Supply-chain integrity

- **Problem:** 2 of 2 cross-origin scripts (jsDelivr `iframemanager` and `cookieconsent`) lack an `integrity` attribute, so a CDN compromise would execute arbitrary code.
- **Solution:**
  - Pin exact versions and add SRI hashes:

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

  - Better still, self-host these two libraries so they fall under your own cache and CSP.

3D. Reduce technology disclosure and move the login path `Best Practices`

- **Impact:** Attack-surface enumeration
- **Problem:** The `server: Apache` header discloses the stack, and the WordPress login form is served on the default `/wp-login.php` path (flagged as a warn).
- **Solution:**
  - Suppress the version banner: `ServerTokens Prod` and `ServerSignature Off` in Apache.
  - Restrict or rename the login entry point (e.g. a WAF rule or a plugin that moves `/wp-login.php`), and add rate limiting plus 2FA.

3E. Drop legacy JavaScript polyfills `Performance`

- **Impact:** Bundle size, TBT
- **Problem:** PSI's `legacy-javascript-insight` estimates 12 KiB of savings from transpiled/polyfilled code shipped to modern browsers.
- **Solution:**
  - Build with `browserslist` targeting modern evergreen browsers and emit a separate legacy bundle via `module` / `nomodule`.
  - Remove unused jQuery Migrate if the theme no longer depends on deprecated jQuery APIs.

3F. Strengthen the Content-Security-Policy `Security`

- **Impact:** XSS defense-in-depth
- **Problem:** CSP is present but only `frame-ancestors 'self';` — `default-src` is missing and `object-src` is not `'none'`. Site signals show no auth, payments,

user content, or commerce, so XSS attack surface is minimal and this is calibrated to P3.

- **Solution:** If you later add login or user content, deploy a nonce-based policy rather than a flat allowlist:

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

  For a brochure/docs page as-is, this is lower value than the P1/P2 items above.

3G. Complete advanced header hardening (HSTS preload, COOP, CORP) `Security`

- **Impact:** Transport hardening, origin isolation
- **Problem:** HSTS lacks the `preload` directive, and Cross-Origin-Opener-Policy and Cross-Origin-Resource-Policy are both missing.
- **Solution:**

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

  Submit the domain at hstspreload.org once the preload directive is live.

3H. Reduce technology disclosure and move the login off the default path `Security`

- **Impact:** Attack-surface reduction
- **Problem:** The `Server: Apache` header discloses the web server, and the WordPress login form is served on the default `/wp-login.php` path.
- **Solution:**
  - Suppress the banner: `ServerTokens Prod` and `ServerSignature Off` in Apache config.
  - Move the login to a custom slug (e.g. via a security plugin or `wp-login.php` rewrite) and add rate limiting / 2FA.

3I. Fix structured data and vague repeated link text `SEO`

- **Impact:** Rich results eligibility, link-purpose clarity
- **Problem:** PSI's `structuredData` audit fails and the single JSON-LD block has type `Unknown`; 10 link texts repeat verbatim (e.g. "home" ×2, "contact" ×2, "play and nope alliance logo" ×2).

- **Solution:**
  - Replace the untyped JSON-LD with a valid `@type` (e.g. `Organization`, `WebSite`, or `WebPage`) and validate in the Rich Results Test.
  - Disambiguate repeated nav/footer links with `aria-label` or visually-hidden context, e.g. `<a href="/contact" aria-label="Contact – footer">Contact</a>`.

3J. Optimize font delivery `Performance`

- **Impact:** Page weight, FCP
- **Problem:** Fonts are the largest resource type at 105.3 KB across 3 files — 40% of the 262.5 KB total page weight.
- **Solution:**
  - Subset to the glyphs actually used (Latin + punctuation).
  - Preload the primary weight: `<link rel="preload" as="font" type="font/woff2" href="…" crossorigin>`.
  - Consider `font-display: swap` and dropping unused weights/styles.

3K. Verify color contrast and link distinguishability `Accessibility`

- **Impact:** WCAG 1.4.3, 1.4.1
- **Problem:** axe could not determine contrast on 10 nodes and flagged 1 node for `link-in-text-block`; PSI also fails `presentation-role-conflict` on the reCAPTCHA iframe.
- **Solution:**
  - Manually check the 10 unresolved contrast nodes (likely gradient/alpha backgrounds) against 4.5:1 for body text and 3:1 for large text.
  - Underline in-text links or add a non-color affordance.
  - Remove `role="presentation"` from the reCAPTCHA iframe wrapper if it conflicts with the iframe's own semantics.

3L. Fix tap targets and add structured data `SEO`

- **Impact:** Mobile usability, rich results
- **Problem:** PSI reports failing `tapTargets` and `structuredData` audits; the JSON-LD block is present but its type is reported as Unknown.
- **Solution:**
  - Ensure interactive elements are at least 24×24 px with adequate spacing (WCAG 2.5.8).

- Replace the generic JSON-LD with a typed schema (`Organization` , `LocalBusiness` , or `ContactPage`) and validate with Google's Rich Results Test.

3M. Cache the HTML document `Performance`

- **Impact:** Repeat-visit TTFB, LCP
- **Problem:** The document response sets `cache-control: max-age=0` with an `expires` timestamp in the past, so every navigation re-fetches the HTML; PSI's `cache-insight` flags ~1 KiB of savings.
- **Solution:**
  - Configure WP Rocket to serve cached HTML with a short `max-age` (e.g. 600) plus `stale-while-revalidate` .
  - Keep the contact page dynamic only if form tokens require it; otherwise cache and hydrate the form client-side.

3N. Add COOP, CORP and X-Permitted-Cross-Domain-Policies `Security`

- **Impact:** Origin isolation, cross-origin read protection
- **Problem:** Cross-Origin-Opener-Policy and Cross-Origin-Resource-Policy are missing, and X-Permitted-Cross-Domain-Policies is unset. Site signals show no auth, payments, user content or e-commerce, so exploitation value is low.
- **Solution:**

  ```
  Cross-Origin-Opener-Policy: same-origin
  Cross-Origin-Resource-Policy: same-origin
  X-Permitted-Cross-Domain-Policies: none
  ```

  Low-cost hardening; not urgent for a brochure-style agency page.

3O. Trim image delivery (est. 110 KiB) `Performance`

- **Impact:** Page weight, LCP
- **Problem:** PSI's `image-delivery-insight` estimates 110 KiB of savings, and the runtime capture shows 8 image requests totalling 287.5 KB out of 560.6 KB total.
- **Solution:**
  - Serve modern formats (WebP/AVIF) with `<picture>` fallbacks.
  - Right-size images to their rendered dimensions and add `srcset` where missing.
  - Note: the HTML inventory sees 44 SVG `<img>` elements, so verify which raster assets the 287.5 KB actually comes from (likely CSS backgrounds or the OG image).

3P. Disambiguate repeated link text `SEO`

- **Impact:** Link-purpose clarity, screen-reader navigation
- **Problem:** The HTML inventory lists repeated vague link text: "home" ×2, "work" ×2, "about" ×2, "contact" ×2, "design & innovation" ×2, "business transformation" ×2, "technical maintenance" ×2, and "play and nope alliance logo" ×2.
- **Solution:**
  - Give each duplicate link a distinct accessible name via `aria-label` or visually-hidden text, e.g. `<a href="/work" aria-label="View our work">work</a>`.
  - For the logo link, use `aria-label="Play and Nope Alliance — home"` on one and a distinct label on the other.

3Q. Address failing tapTargets and structuredData audits `SEO`

- **Impact:** Mobile usability, rich-result eligibility
- **Problem:** PSI lists two failing modeled SEO audits: `tapTargets` and `structuredData`. The page's single JSON-LD block is typed "Unknown", so it is unlikely to produce rich results.
- **Solution:**
  - Ensure interactive targets are at least 24×24 px with adequate spacing (WCAG 2.5.8).
  - Replace the untyped JSON-LD with a valid `Organization` / `LocalBusiness` schema including `name`, `url`, `logo`, `address` and `sameAs`.

3R. Suppress the Server header `Security`

- **Impact:** Technology fingerprinting
- **Problem:** The response discloses `Server: Apache`, and Security basics flags 'Technology disclosure — warn'.
- **Solution:**

  ```
  ServerTokens Prod
  ServerSignature Off
  Header unset Server
  ```

  Or strip the header at the CDN/reverse proxy.

3S. Enable browser caching for the document `Performance`

- **Impact:** Repeat-visit load time
- **Problem:** The document is served with `cache-control: max-age=0` (and a matching `expires` in the past), so repeat visitors revalidate every navigation;

PSI's `cache-insight` estimates 1 KiB savings.

- **Solution:**
  - In WP Rocket, enable browser caching and set a long `max-age` for static assets (e.g. 1 year) while keeping HTML short-lived.
  - Add `Cache-Control: public, max-age=31536000, immutable` for hashed theme/plugin assets.

3T. Complete advanced header hardening `Security`

- **Impact:** Origin isolation, HSTS preload eligibility
- **Problem:** HSTS lacks `preload`, COOP and CORP are missing, `X-Permitted-Cross-Domain-Policies` is absent, and the `Server: Apache` header discloses the stack.
- **Solution:**
  - Add `preload` to HSTS and submit to hstspreload.org:

```
Strict-Transport-Security: max-age=31536000; includeSubDomains;
preload
```

  - Set `Cross-Origin-Opener-Policy: same-origin` and `Cross-Origin-Resource-Policy: same-origin`.
  - Set `X-Permitted-Cross-Domain-Policies: none`.
  - Suppress the `Server` header (`ServerTokens Prod` / `Header unset Server`).

3U. Fix the reCAPTCHA presentation-role conflict `Accessibility`

- **Impact:** WCAG 4.1.2
- **Problem:** axe reports 1 minor `presentation-role-conflict` violation on `iframe[title="reCAPTCHA"]` — an element marked presentational is still exposed.
- **Solution:**
  - Remove the conflicting `role="presentation"` / `role="none"` from the reCAPTCHA iframe wrapper, or ensure the iframe is genuinely hidden from the accessibility tree.
  - This is a third-party widget; if it cannot be patched, document it as a known upstream issue.