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: 77 / 100
Status: □ □ **Needs Improvement**

Site overall 77 is the mean of 5 pages. Scores range 70 (https://playandnope.com/) → 88 (https://playandnope.com/full-stack-digital-agency). Weakest page: PSI mobile 73 / desktop 82 with a severe mobile LCP of 7.4 s (desktop 0.6 s) and a desktop CLS of 0.367 — two heavy-penalty CWV failures that dominate the score. TBT (0–1 ms), TTFB (38 ms) and FCP (1.81 s mobile) are all healthy, so the problem is critical-path/LCP delivery rather than server or main-thread cost. Accessibility is otherwise excellent (PSI 100/100, 37 axe passes) with a single serious color-contrast violation on `.menu-item-75 > .navigation__description`. Image assets are clean — 30 images, 0 missing alt, 0 missing lazy loading, mostly SVG — so the image budget contributes little drag. Security basics PASS, but CSP is `frame-ancestors 'self';` only, HSTS lacks preload, COOP/CORP are missing and 2 cross-origin jsdelivr scripts lack SRI. W3C validation failed with HTTP 429, so HTML validity is unscored and confidence is medium.

Per-page scores

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

Score	Performance	Accessibility	Best Practices	SEO	Security
70	73	100	100	92	PASS

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

Score	Performance	Accessibility	Best Practices	SEO	Security
88	93	100	100	100	PASS

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

Score	Performance	Accessibility	Best Practices	SEO	Security
70	59	99	96	100	PASS

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

Score	Performance	Accessibility	Best Practices	SEO	Security
88	96	98	100	100	PASS

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

Score	Performance	Accessibility	Best Practices	SEO	Security
70	61	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/	**73** / 82	**7.40 s** / 602 ms	0.000 / **0.367**
https://playandnope.com/privacy-policy	**93** / 97	**2.49 s** / 601 ms	0.089 / **0.098**
https://playandnope.com/contact	59 / **57**	**6.00 s** / 1.16 s	0.056 / **0.257**

URL	Performance (M / D)	LCP (M / D)	CLS (M / D)
https://playandnope.com/full-stack-digital-agency	**96** / 98	**2.49 s** / 634 ms	0.000 / **0.084**
https://playandnope.com/digital-solutions-contact	**61** / 71	**6.38 s** / 1.72 s	0.056 / **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. Fix mobile LCP (7.4 s) — critical path and LCP resource delivery `Performance`

- **Impact:** LCP, Speed Index, TTI
- **Problem:** Mobile LCP is 7.4 s versus 0.6 s on desktop, with `network-dependency-tree-insight` scoring 0.00 and `interactive` at 7.4 s. The 6.8 s mobile/desktop delta points to a delivery problem, not a rendering one.
- **Solution:**
  - Identify the LCP element in DevTools Performance panel and preload it:

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

  - Self-host the 3 font files (105.3 KB) and preload the one used above the fold; add `font-display: swap`.
  - Flatten the critical request chain flagged by `network-dependency-tree-insight` — inline critical CSS and defer the rest.
  - Remove legacy JS polyfills (`legacy-javascript-insight`, est. 12 KiB savings).

1B. Fix desktop CLS 0.367 — reserve space for images `Performance`

- **Impact:** CLS
- **Problem:** Desktop CLS is 0.367 (mobile 0.000) and 5 images lack explicit width/height attributes, which lets late-loading content push the layout.
- **Solution:**
  - Add `width` / `height` (or `aspect-ratio`) to the 5 images missing dimensions:

```
<img src="…" width="360" height="270" alt="…" loading="lazy">
```

  - For responsive containers use CSS `aspect-ratio` so the box is reserved before the asset loads.
  - Re-measure CLS on desktop after the change — the mobile/desktop divergence suggests a viewport-specific layout shift.

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

- **Impact:** WCAG 1.4.3 (AA), axe serious violation
- **Problem:** axe reports 1 serious `color-contrast` violation on `.menu-item-75 > .navigation__description`, plus 8 nodes axe could not determine (alpha/gradient backgrounds).
- **Solution:**
  - Raise the text/background contrast to at least 4.5:1 for normal text (3:1 for ≥18.66 px bold or ≥24 px).
  - Manually verify the 8 'incomplete' nodes — axe skips elements with alpha-transparency or gradients.
  - Also check the `link-in-text-block` incomplete node so links are distinguishable without relying on color alone (add underline or a non-color cue).

1D. Set a real Cache-Control max-age on the document `Performance`

- **Impact:** Repeat-visit TTFB, document latency
- **Problem:** The document response sets `cache-control: max-age=0` with `expires` in the past, forcing revalidation on every visit; the document request is the slowest resource at 550 ms.
- **Solution:** Serve the HTML with a positive max-age and stale-while-revalidate so repeat visitors get a cached copy:

  ```
  Cache-Control: public, max-age=3600, stale-while-revalidate=86400
  ```

  WP Rocket can set this under Cache → Browser Cache; verify the header on the canonical URL after deploy.

1E. 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`; 9 more nodes are flagged as incomplete.
- **Solution:**
  - Raise the text color to at least 4.5:1 against its background (or 3:1 for large text ≥18.66 px bold / 24 px).
  - Verify with the DevTools contrast checker, then re-run axe to clear the 9 incomplete nodes.

- If the descriptions are decorative, consider `aria-hidden="true"` instead of recoloring.

1F. Cut reCAPTCHA's JavaScript cost `Performance`

- **Impact:** TBT, TTI, INP, total page weight
- **Problem:** reCAPTCHA pulls 1.43 MB from gstatic.com (11 requests) with 176+170+170 KB flagged as unused JS and long tasks of 283/278/215/191/187 ms. TBT is 666 ms mobile / 798 ms desktop and TTI is 11.4 s.
- **Solution:**
  - Lazy-load reCAPTCHA only when the user focuses the form, instead of on page load.
  - Evaluate a lighter alternative (Cloudflare Turnstile, hCaptcha) or a honeypot + server-side rate limit for a low-risk contact form.
  - If you keep reCAPTCHA, load it with `defer` and gate the Gravity Forms submit handler on the token callback so the main thread isn't blocked during initial render.

1G. Fix the 6.0 s mobile LCP `Performance`

- **Impact:** LCP, FCP, Speed Index
- **Problem:** Mobile LCP is 6.0 s and FCP 1.97 s, while desktop LCP is 1.2 s and FCP 545 ms — the gap is mobile-specific and points at main-thread contention rather than server latency (TTFB is 44 ms mobile / 3 ms desktop).
- **Solution:**
  - Identify the LCP element in DevTools Performance and preload it (`<link rel="preload" as="image" fetchpriority="high">`).
  - Ensure the hero is not `loading="lazy"` and is not injected by JS after hydration.
  - Reduce main-thread work from reCAPTCHA (see the P1 fix above) — the 283 ms long task lands inside the LCP window.

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

- **Impact:** XSS defense-in-depth
- **Problem:** The CSP is `frame-ancestors 'self';` only — no `default-src` and no `object-src 'none'` , so it restricts framing but nothing else. The page contains a user-input textarea, so injected script would persist into submitted content.
- **Solution:** 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';
```

Roll it out in report-only mode first to catch the jsdelivr and gstatic dependencies.

1I. Defer or lazy-load reCAPTCHA to fix mobile LCP of 6.4 s `Performance`

- **Impact:** LCP, TBT, FCP, Speed Index, page weight
- **Problem:** Mobile LCP is 6.4 s (desktop 1.7 s) and reCAPTCHA accounts for 1.42 MB across 10 requests from www.gstatic.com, with 176+170+170 KB of unused JS and long tasks up to 238 ms.
- **Solution:** Load reCAPTCHA only when the user interacts with the form, not on page load:
  - Gravity Forms: enable the reCAPTCHA v3 'defer' / 'only load when needed' option, or switch to a honeypot / Turnstile alternative.
  - If you must keep v3, inject `https://www.google.com/recaptcha/api.js?render=explicit` on first focus of the form and call `grecaptcha.execute()` on submit.
  - Verify the LCP element in DevTools Performance panel — if it is the hero, ensure it is not blocked behind the reCAPTCHA script chain.

1J. Harden CSP with default-src, object-src 'none', and nonce + strict-dynamic `Security`

- **Impact:** XSS defense-in-depth on a page that accepts user input
- **Problem:** CSP is only `frame-ancestors 'self';` — no `default-src`, no `object-src 'none'`, and no script/resource restrictions. The page contains a `<textarea>` (user-generated content signal), so XSS would persist into stored content.
- **Solution:** Deploy a nonce-based CSP rather than a flat allowlist:

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

  - Generate a fresh nonce per response and add it to every `<script>` tag.
  - Keep `frame-ancestors 'self'` (already present) and add `object-src 'none'` and `default-src 'self'` as the baseline.

Priority 2: Important

Essential for compliance, user reach, and search visibility.

2A. Harden CSP — add default-src and object-src 'none' `Security`

- **Impact:** XSS defense-in-depth
- **Problem:** CSP is `frame-ancestors 'self';` only — no `default-src` and no `object-src 'none'`, so no script or resource restrictions are enforced. The site runs WordPress with a login form served on `/wp-login.php`, so an auth surface does exist despite the heuristic signals.
- **Solution:** 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';
```

  - Start in `Content-Security-Policy-Report-Only` to collect violations, then enforce.
  - Note the two jsdelivr scripts (`iframemanager.js`, `cookieconsent.umd.js`) will need nonces or hashes.

2B. Add SRI to cross-origin scripts `Security`

- **Impact:** Supply-chain integrity
- **Problem:** 2 of 2 cross-origin scripts lack an `integrity` attribute — both are loaded from `cdn.jsdelivr.net` (iframemanager.js, cookieconsent.umd.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 hashes with `openssl dgst -sha384 -binary file.js | openssl base64 -A`.
  - Better still, self-host these two libraries to remove the third-party origin entirely.

2C. Add HSTS preload directive `Security`

- **Impact:** Transport security, preload eligibility
- **Problem:** HSTS is `max-age=31536000; includeSubDomains` but lacks the `preload` directive, so the domain cannot be submitted to the preload list.
- **Solution:**

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

  - Verify all subdomains serve HTTPS before submitting at hstspreload.org.

2D. Fix document cache-control max-age=0 `Performance`

- **Impact:** Repeat-visit TTFB, LCP
- **Problem:** The document response sets `cache-control: max-age=0` with `expires` equal to the request time, forcing revalidation on every visit even though WP Rocket is active.
- **Solution:**
  - Set a short but non-zero browser TTL and a longer shared-cache TTL 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 (WP Rocket does this by default).
  - Confirm the canonical URL is warmed after deploy so the first visitor does not pay the cold-start cost.

2E. Replace vague and repeated link text `SEO`

- **Impact:** SEO link-text audit, screen-reader link purpose
- **Problem:** The `link-text` SEO audit scores 0.00 with 4 links lacking descriptive text, and 'read more' is repeated ×4 across the page.
- **Solution:**
  - Replace 'read more' with the destination, e.g. `<a href="/work/acme">Read the Acme case study</a>`.
  - Where the visible label must stay short, disambiguate with `aria-label` or visually-hidden text:

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

  - Apply the same to the repeated 'design & innovation', 'development' and 'technical maintenance' links.

2F. Fix tap targets and add valid structured data `SEO`

- **Impact:** SEO score (92), mobile usability, rich results

- **Problem:** PSI reports failing SEO audits `tapTargets` and `structuredData`; the single JSON-LD block is typed 'Unknown'.
- **Solution:**
  - Ensure every interactive element is at least 48×48 px with adequate spacing (WCAG 2.5.8 minimum is 44×44 px).
  - Replace the untyped JSON-LD block with a valid schema.org type, e.g.:

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

  - Validate with Google's Rich Results Test.

2G. Reserve space for the cookie consent banner `Performance`

- **Impact:** CLS (0.089 mobile / 0.098 desktop)
- **Problem:** The only layout-shift source is `body.privacy-policy > div#cc-main > div.cm-wrapper > div.cm` (shift 0.089) — the cookie banner injects after first paint.
- **Solution:**
  - Pre-allocate the banner's footprint with a fixed-height placeholder or `min-height` on `#cc-main` before the consent script runs.
  - Load the cookieconsent CSS/JS eagerly (or inline the critical CSS) so the banner renders in the first paint.
  - Alternatively, render the banner server-side and only hydrate the buttons client-side.

2H. Reduce document latency `Performance`

- **Impact:** FCP (2.02 s mobile), document latency
- **Problem:** PSI flags `document-latency-insight` as high priority with an estimated 520 ms savings; the document request took 550 ms in the browser capture.
- **Solution:**
  - Enable full-page caching for the privacy policy (WP Rocket is already installed — confirm the page is in the cache and warmed).
  - Add a CDN in front of the origin to cut round-trip time.
  - Check for slow plugins or DB queries on this template via Query Monitor.

2I. Eliminate forced reflow `Performance`

- **Impact:** Main-thread work, FCP

- **Problem:** PSI flags `forced-reflow-insight` as high priority (score 0.00) — layout is being read after a DOM mutation, forcing synchronous reflow.
- **Solution:**
  - Batch DOM reads before writes; avoid interleaving `offsetWidth` / `getBoundingClientRect` with style mutations.
  - Use `requestAnimationFrame` for measurement, then apply writes in a separate frame.
  - Audit theme JS (`global.*.min.js` , `core.*.min.js`) for layout-thrashing patterns.

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

- **Impact:** Supply-chain integrity for jsdelivr assets
- **Problem:** 2 of 2 cross-origin scripts from cdn.jsdelivr.net lack an `integrity` attribute, so a compromised CDN could inject arbitrary JS.
- **Solution:** Pin a 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. Replace the default WordPress meta description `SEO`

- **Impact:** Search snippet CTR
- **Problem:** The meta description is the WordPress default: "Our website address is: https://playandnope.com." — it does not describe the page.
- **Solution:**
  - Set a unique 120–160 character description per page via Yoast/Rank Math.
  - For the privacy policy, summarize what data is collected and how it is used.

2L. Enlarge tap targets `Accessibility`

- **Impact:** Mobile usability, WCAG 2.5.8
- **Problem:** PSI's modeled `tapTargets` audit fails on mobile.
- **Solution:**
  - Ensure every interactive element is at least 44×44 px (or 24×24 px with sufficient spacing).

- Add padding to nav links and icon buttons rather than relying on the icon's intrinsic size.

2M. Remove the /contact → /digital-solutions-contact/ redirect `Performance`

- **Impact:** TTFB, LCP, document latency
- **Problem:** The slowest-request list shows 480 ms for the `/contact` redirect hop plus 325 ms for the final document, matching the 530 ms `document-latency-insight` estimated savings.
- **Solution:**
  - Link directly to `https://playandnope.com/digital-solutions-contact/` in navigation and internal links.
  - Or serve the contact page at `/contact` and 301 the long slug, so the canonical URL is the short one.

2N. Resolve the 5 console errors `Best Practices`

- **Impact:** Best Practices score, form reliability
- **Problem:** PSI flags `errorsInConsole` as a failing audit. The runtime capture shows a CORS block on `recaptcha/.../styles__ltr.css`, two `requestStorageAccess: Permission denied` errors, and a `net::ERR_FAILED` on the same stylesheet.
- **Solution:**
  - The CORS failure is inside Google's own reCAPTCHA iframe and is usually triggered by a cookie-consent script blocking storage before reCAPTCHA initialises — load the consent manager before `api.js`.
  - Verify the reCAPTCHA site key is valid for this domain and that the widget is not being re-initialised twice.
  - Re-run the runtime capture after the fix to confirm zero console errors.

2O. Resolve the unresolved color-contrast and link-in-text-block checks `Accessibility`

- **Impact:** WCAG 1.4.3, 1.4.1
- **Problem:** axe could not determine contrast for 10 nodes and flagged 1 node for `link-in-text-block`; the audit reports 1 minor violation and 48 passes, so these are the only accessibility gaps on an otherwise 99/100 page.
- **Solution:**
  - Manually check the 10 flagged nodes (axe skips alpha-transparency and gradients) and raise any below 4.5:1 for body text / 3:1 for large text.

    - Underline in-text links or add a non-color affordance so they are distinguishable without relying on hue.

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

- **Impact:** WCAG 1.3.1, 4.1.2
- **Problem:** The contact form's textarea has no label, while the other three visible fields are labeled.
- **Solution:**

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

  If the design hides the label visually, keep it in the DOM and use a visually-hidden class rather than removing it.

2Q. Add the HSTS preload directive `Security`

- **Impact:** Transport security
- **Problem:** HSTS is `max-age=31536000; includeSubDomains` but lacks `preload`, and the security-basics table marks HSTS preload as fail.
- **Solution:**

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

  Then submit the domain at hstspreload.org. Note this is a long-term commitment — confirm every subdomain serves HTTPS first.

2R. Fix structured data and tap targets `SEO`

- **Impact:** Rich results eligibility, mobile usability
- **Problem:** PSI flags `structuredData` and `tapTargets` as failing modeled SEO audits. The page has 1 JSON-LD block but its type resolves to "Unknown".
- **Solution:**
    - Replace the untyped JSON-LD with a valid `Organization` / `LocalBusiness` / `ContactPage` graph including `name`, `url`, `logo`, and `contactPoint`.
    - Enlarge tap targets to at least 48×48 px with adequate spacing — the 43 anchors include dense footer and nav links.

2S. Cut image delivery weight (~460 KiB) `Performance`

- **Impact:** LCP, page weight, mobile FCP

- **Problem:** PSI's `image-delivery-insight` estimates 460 KiB of savings, and the runtime capture shows 8 image requests totalling 287.5 KB — including JPEGs such as `sample-image-1024x337.jpg` (39.4 KB) and `img-03-388x530.jpg` (58.4 KB) — while the HTML inventory sees only 44 SVG placeholders, meaning the raster images are being served outside the `<img>`/srcset path.
- **Solution:**
  - Serve WebP/AVIF with a `<picture>` fallback for the JPEGs identified in the network capture.
  - Ensure the LCP image is preloaded and **not** lazy-loaded; keep `loading="lazy"` only for below-the-fold images.
  - If the JPEGs are CSS `background-image`s, move them to real `<img>` elements so srcset/sizes and lazy-loading apply.

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

- **Impact:** FCP, Speed Index, main-thread work
- **Problem:** PSI flags `forced-reflow-insight` **(high)** and `document-latency-insight` with an estimated 510 ms of savings; the runtime capture shows the document request taking 493 ms, and mobile FCP is 1.96 s versus 554 ms on desktop.
- **Solution:**
  - Audit scroll/resize handlers and layout reads interleaved with style writes; batch reads before writes and cache layout values.
  - Reduce the critical-path document work: the HTML is 195 KB and the decoded body is 210 KB — trim inline markup and defer non-critical work.
  - Consider warming the page cache (WP Rocket is active) so the first visitor does not pay the cold-start cost.

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

- **Impact:** WCAG 1.3.1, screen-reader navigation
- **Problem:** The heading outline jumps from h1 "Get to know us" straight to h3 "Full-stack digital agency powered by curiosity"; PSI's `heading-order` audit scores 0.00 (weight 3) and axe flags `.hero__description > h3`.
- **Solution:** Change the hero sub-heading to `<h2>` (or promote the h1 to a visually-styled h2 if the design requires the smaller size), then re-check the full outline — the page currently has h1 ×1, h2 ×7, h3 ×12.

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

- **Impact:** XSS defense-in-depth

- **Problem:** The CSP is only `frame-ancestors 'self';` — it is missing `default-src` and `object-src 'none'`, so it provides no script or resource restrictions (advanced-tier CSP check: fail).
- **Solution:** Extend the existing header rather than replacing it with a flat allowlist:

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

  Site signals show no auth, payments, or user-generated content, so this is defense-in-depth rather than an urgent exposure — but the change is a one-liner.

2W. Reduce Total Blocking Time (506 ms mobile) `Performance`

- **Impact:** TBT, INP, Time to Interactive (11.5 s)
- **Problem:** TBT is 506 ms mobile / 456 ms desktop, with 10 long tasks all originating from `recaptcha__en.js` (238 ms, 225 ms, 208 ms, 170 ms, …) and Time to Interactive at 11.5 s.
- **Solution:**
  - Apply the reCAPTCHA deferral above; it removes the bulk of the long tasks.
  - Audit the 42 scripts on the page (16 defer, 1 async, 2 render-blocking) and drop any Gravity Forms / jQuery plugins not needed on this contact page.
  - Consider `requestIdleCallback` or dynamic `import()` for non-critical theme scripts.

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

- **Impact:** Best Practices score, console cleanliness
- **Problem:** 5 console events including `requestStorageAccess: Permission denied` (×2), a CORS-blocked XHR to `styles__ltr.css`, and `net::ERR_FAILED` on the same stylesheet. PSI flags `errorsInConsole` as a failing audit.
- **Solution:**
  - Update the reCAPTCHA integration to the current version — the `styles__ltr.css` CORS failure is a known issue with older reCAPTCHA builds.
  - If the errors persist, switch to reCAPTCHA v3 with `render=explicit` and load it after user interaction.
  - Re-run the audit after the change to confirm `errorsInConsole` passes.

2Y. Add HSTS preload, COOP, and CORP headers `Security`

- **Impact:** Transport security, origin isolation
- **Problem:** HSTS is `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=63072000; includeSubDomains;
preload
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
```

  - Submit the domain to hstspreload.org after confirming the preload directive is live.

Priority 3: Best Practice

Recommended for long-term maintainability.

3A. Add COOP and CORP headers `Security`

- **Impact:** Origin isolation, cross-origin read protection
- **Problem:** `Cross-Origin-Opener-Policy` and `Cross-Origin-Resource-Policy` are both missing from the response.
- **Solution:**

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

  - Low risk for a marketing site with no auth or payments, but cheap to add.

3B. Reduce technology disclosure and harden WordPress login `Security`

- **Impact:** Attack-surface reduction
- **Problem:** `Server: Apache` discloses the web server, `X-Permitted-Cross-Domain-Policies` is missing, and the login form is served on the default `/wp-login.php` path.
- **Solution:**
  - Suppress the banner: `ServerTokens Prod` and `ServerSignature Off` in Apache config.
  - Add `X-Permitted-Cross-Domain-Policies: none`.
  - Move the login to a custom path, add rate limiting / CAPTCHA, and enable 2FA for admin accounts.

3C. Tighten the Content-Security-Policy `Security`

- **Impact:** XSS defense-in-depth
- **Problem:** CSP is present but only sets `frame-ancestors 'self'` — `default-src` is missing and `object-src` is not `'none'`. Site signals show no auth, payments, or user content, so XSS attack surface is low.
- **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 site as-is, prioritize the P1/P2 items above first.

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

- **Impact:** Cross-origin isolation
- **Problem:** Both COOP and CORP headers are missing. The site has no auth or payments, so the risk is low.
- **Solution:**

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

3E. Add the HSTS preload directive `Security`

- **Impact:** HSTS preload list eligibility
- **Problem:** HSTS is set with `max-age=31536000; includeSubDomains` but lacks `preload`.
- **Solution:**

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

  Then submit the domain at hstspreload.org.

3F. Drop legacy JavaScript polyfills `Performance`

- **Impact:** JS bytes (12 KiB est. savings)
- **Problem:** PSI's `legacy-javascript-insight` estimates 12 KiB of savings; scripts total 103.6 KB across 8 requests.
- **Solution:**
  - Configure your bundler's `browserslist` to modern targets only.

- Remove `@babel/preset-env` polyfills for features supported by your target browsers.

3G. Optimize web fonts `Performance`

- **Impact:** Page weight (105.3 KB fonts)
- **Problem:** 3 font files account for 105.3 KB — the largest single resource type on the page, larger than scripts (103.6 KB).
- **Solution:**
  - Subset fonts to the glyphs actually used.
  - Serve WOFF2 only and drop legacy WOFF/TTF fallbacks.
  - Add `<link rel="preload" as="font" type="font/woff2" crossorigin>` for the primary face.

3H. Suppress the Server header `Security`

- **Impact:** Information disclosure
- **Problem:** The response discloses `Server: Apache`, which the security basics check flags as a warn.
- **Solution:**

```
ServerTokens Prod
ServerSignature Off
```

3I. Move the WordPress login off /wp-login.php `Security`

- **Impact:** Brute-force / credential-stuffing surface
- **Problem:** Security basics flags the login form on the default `/wp-login.php` path.
- **Solution:**
  - Rename the login URL (e.g. WPS Hide Login) or restrict `/wp-login.php` by IP.
  - Add rate limiting and 2FA for admin accounts.

3J. Add valid structured data `SEO`

- **Impact:** Rich results eligibility
- **Problem:** PSI's modeled `structuredData` audit fails; the single JSON-LD block is typed "Unknown".
- **Solution:**
  - Add `Organization` and `WebSite` schema on the homepage and `WebPage` on this page.

- Validate with Google's Rich Results Test and the Schema Markup Validator.

3K. 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.
- **Solution:**
  - Strip or genericise the banner: `ServerTokens Prod` and `ServerSignature Off` in Apache.
  - Move the login to a custom path via a security plugin, and add rate limiting plus 2FA on `/wp-login.php`.

3L. Cache the HTML document at the edge `Performance`

- **Impact:** TTFB, repeat-visit LCP
- **Problem:** The document response sets `cache-control: max-age=0` with an `expires` timestamp in the past, even though WP Rocket is detected. PSI's `cache-insight` estimates only 1 KiB of savings, so the impact is modest.
- **Solution:**
  - Confirm WP Rocket's page cache is actually serving the HTML (check for the `<!-- This is WP Rocket -->` footer marker on a cold visit).
  - If a CDN sits in front, set a short edge TTL (e.g. `s-maxage=600`) with `stale-while-revalidate` so repeat visitors skip the origin round trip.

3M. Fix the presentation-role-conflict on the reCAPTCHA iframe `Accessibility`

- **Impact:** WCAG 4.1.2
- **Problem:** axe reports 1 minor violation: `iframe[title="reCAPTCHA"]` has a conflicting `role="none"` / `role="presentation"`.
- **Solution:** Remove the presentational role from the reCAPTCHA iframe, or add `aria-hidden="true"` if it is genuinely decorative — but keep the `title` attribute so the widget remains announced.

3N. Disambiguate repeated link text `SEO`

- **Impact:** Anchor-text quality, screen-reader navigation
- **Problem:** The HTML inventory lists 10 repeated link labels, including "info@playandnope.com" ×3, "home" ×2, "work" ×2, and "contact" ×2.
- **Solution:**
  - Add `aria-label` or visually-hidden context to repeated anchors, e.g. `<a href="/work/">Work<span class="sr-only"> — our portfolio</span>`

`</a>`.

- Keep the visible label short but make the accessible name unique per destination.

3O. Add HSTS preload, COOP, CORP, and SRI `Security`

- **Impact:** Transport hardening, origin isolation, third-party script integrity
- **Problem:** HSTS lacks the `preload` directive, `Cross-Origin-Opener-Policy` and `Cross-Origin-Resource-Policy` are missing, and 2 of 2 cross-origin scripts (from `cdn.jsdelivr.net`) lack `integrity` attributes.
- **Solution:**
  - Add `preload` to HSTS: `Strict-Transport-Security: max-age=31536000; includeSubDomains; preload`, then submit to hstspreload.org.
  - Set `Cross-Origin-Opener-Policy: same-origin` and `Cross-Origin-Resource-Policy: same-origin`.
  - Add `integrity="sha384-…"` (plus `crossorigin="anonymous"`) to the jsDelivr `<script>` tags for iframemanager and cookieconsent.

3P. Add structured data and disambiguate repeated link text `SEO`

- **Impact:** Rich results eligibility, link-purpose clarity
- **Problem:** PSI's modeled `structuredData` audit fails and the single JSON-LD block is typed "Unknown"; the inventory also lists 10 link texts repeated twice each (e.g. "work", "about", "contact").
- **Solution:**
  - Replace the unknown JSON-LD with a valid `Organization` / `LocalBusiness` schema including `name`, `url`, `logo`, and `sameAs`.
  - Where repeated link text is genuinely ambiguous (e.g. two "contact" links pointing to different targets), disambiguate with `aria-label` or surrounding context.

3Q. Reduce technology disclosure and move login off the default path `Best Practices`

- **Impact:** Attack-surface reduction
- **Problem:** The `Server: Apache` response header discloses the web server, and the WordPress login form is served on the default `/wp-login.php` path (both flagged as warnings).
- **Solution:**
  - Suppress the server banner: `ServerTokens Prod` and `ServerSignature Off` in Apache.

- Move or protect the login: rename the login slug via a security plugin, or restrict `/wp-login.php` by IP / rate limit at the edge.

3R. Fix document cache-control max-age=0 `Performance`

- **Impact:** Repeat-visit TTFB, back/forward cache
- **Problem:** The document response sets `cache-control: max-age=0` with an `expires` timestamp in the past, so the HTML is revalidated on every navigation despite WP Rocket being active.
- **Solution:**
  - In WP Rocket → Cache → Browser Cache, enable HTML browser caching (or set `Cache-Control: public, max-age=600` at the origin).
  - Confirm the canonical URL is warmed after deploy so the first visitor does not pay the cold-start cost.

3S. Fix structured data and tap targets `SEO`

- **Impact:** SEO rich results, mobile usability
- **Problem:** PSI flags `structuredData` and `tapTargets` as failing SEO audits; the single JSON-LD block is reported with type "Unknown".
- **Solution:**
  - Replace the JSON-LD block with a valid `Organization` / `LocalBusiness` schema including `name`, `url`, `logo`, and `contactPoint`.
  - Ensure interactive elements (nav links, form controls) meet the 44×44 px minimum touch target size.

3T. Move login off the default /wp-login.php path and suppress the Server header `Security`

- **Impact:** Brute-force surface, technology disclosure
- **Problem:** The login form is served on the default `/wp-login.php` path, and the `Server: Apache` header discloses the web server.
- **Solution:**
  - Rename the login URL (e.g. WPS Hide Login) and add rate limiting / 2FA.
  - Suppress the version banner:

```
ServerTokens Prod
ServerSignature Off
```