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

Website: https://playandnope.com/
Date: 31.10.2026
Audit Coverage: 100% — all sources returned data
Confidence: high

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: 79 / 100
Status: **Needs Improvement**

Site overall 79 is the mean of 5 pages. Scores range 68 (https://playandnope.com/digital-solutions-contact/) → 86 (https://playandnope.com/industrial-digital-solutions/). Weakest page: Mobile performance is the dominant drag: PSI mobile 56 vs desktop 79, with LCP 5.6 s (desktop 0.5 s), TBT 865 ms and Speed Index 4.21 s — all well past the heavy-penalty thresholds. The cause is concentrated in one third party: reCAPTCHA pulls 1.44 MB from gstatic.com across 10 requests, produces 10 long tasks (253/247/245/235 ms…) and ~520 KB of unused JS, plus a failing styles__ltr.css request that logs CORS and requestStorageAccess console errors. Accessibility is otherwise strong (axe 1 minor violation, 48 passes, Lighthouse a11y 99), though the HTML inventory flags an unlabeled textarea and axe could not resolve 3 color-contrast nodes. Image assets are clean — only 5 SVGs, all with dimensions and lazy loading, so the image budget earns full credit. Security basics returned FAILED: CSP lacks default-src and object-src 'none', HSTS has no preload, COOP/CORP are missing, 3 of 4 cross-origin scripts lack SRI, and WordPress user enumeration is possible — this caps the score below 90. SEO is 100 with valid meta/canonical, offset only by failing tapTargets and an unrecognized JSON-LD type.

Per-page scores

 Needs Improvement · https://playandnope.com/

Score	Performance	Accessibility	Best Practices	SEO	Security
85	99	100	100	92	FAILED

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

Score	Performance	Accessibility	Best Practices	SEO	Security
73	79	100	100	100	FAILED

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

Score	Performance	Accessibility	Best Practices	SEO	Security
68	56	99	96	100	FAILED

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

Score	Performance	Accessibility	Best Practices	SEO	Security
84	93	98	100	100	FAILED

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

Score	Performance	Accessibility	Best Practices	SEO	Security
86	98	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/	99 / **98**	**978 ms** / 445 ms	0.000 / **0.084**

URL	Performance (M / D)	LCP (M / D)	CLS (M / D)
https://playandnope.com/privacy-policy/	**79** / 98	**5.33 s** / 447 ms	0.000 / **0.083**
https://playandnope.com/digital-solutions-contact/	**56** / 79	**5.58 s** / 487 ms	0.000 / **0.083**
https://playandnope.com/real-estate-digital-solutions/	**93** / 98	**2.86 s** / 485 ms	0.000 / **0.083**
https://playandnope.com/industrial-digital-solutions/	98 / 98	**1.95 s** / 485 ms	0.000 / **0.084**

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.
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.

Item	Status	Detail
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:** Credential-stuffing / brute-force attack surface
- **Problem:** The Security basics table reports `User enumeration blocked: fail — WordPress usernames can be enumerated`, and the overall verdict is FAILED.
- **Solution:**
  - Block `?author=N` scans at the web server:

```
RewriteCond %{QUERY_STRING} ^author=([0-9]*) [NC]
RewriteRule ^ - [F,L]
```

  - Restrict the REST users endpoint (`/wp-json/wp/v2/users`) to authenticated requests only.
  - Ensure author archives and the login error message do not reveal whether a username exists.
  - Consider a security plugin (e.g. Wordfence) to enforce both.

1B. Fix the 5.3 s mobile LCP `Performance`

- **Impact:** LCP, Speed Index, TTI
- **Problem:** Mobile LCP is 5.3 s versus 0.4 s on desktop, with a render-blocking insight estimating 730 ms of savings and a failing network-dependency-tree audit.
- **Solution:**
  - Identify the actual LCP element in DevTools Performance (no raster images exist on this page, so it is likely a text block or SVG — check font loading).
  - Preload the LCP font and the LCP element's critical CSS:

```
<link rel="preload" href="/wp-content/themes/.../font.woff2"
as="font" type="font/woff2" crossorigin>
```

- Inline critical CSS and defer the 3 external stylesheets (22.1 KB) so first paint is not blocked.
- Shorten the critical request chain: the theme's `runtime` → `core` → `jquery` → `global` script sequence is serialized; bundle or drop jQuery Migrate if unused.
- Re-test on throttled mobile after each change; target LCP ≤2.5 s.

1C. Stop reCAPTCHA from dominating the main thread `Performance`

- **Impact:** TBT, LCP, Speed Index, total page weight
- **Problem:** reCAPTCHA accounts for 1.44 MB of the 1.91 MB page (10 requests from www.gstatic.com), ~520 KB of unused JS, and 10 long tasks up to 253 ms — driving mobile TBT to 865 ms.
- **Solution:**
  - Load reCAPTCHA only when the user interacts with the form (lazy render on focus), not on page load.
  - Consider replacing it with Cloudflare Turnstile or a honeypot + server-side rate limit — both are far lighter.
  - If keeping reCAPTCHA, use `render=explicit` and call `grecaptcha.render()` on form focus.
  - Fix the failing `styles__ltr.css` request (`net::ERR_FAILED` , CORS-blocked) so the widget doesn't retry.

1D. Cut render-blocking scripts and prioritize the LCP resource `Performance`

- **Impact:** LCP, FCP, Speed Index
- **Problem:** Mobile LCP is 5.6 s against 0.5 s on desktop, with 11 render-blocking scripts out of 40 total and 2 blocking scripts in `<head>` (iframemanager.js, cookieconsent.umd.js from cdn.jsdelivr.net).
- **Solution:**
  - Add `defer` to the two jsdelivr scripts in `<head>` (or move them to the footer).
  - Inline critical above-the-fold CSS and load the rest asynchronously.
  - Preload the actual LCP element (identify it in DevTools Performance panel — the page has only SVGs, so it may be a text block or inline SVG).
  - Audit the 11 render-blocking scripts and defer everything not needed for first paint.

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

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

- **Problem:** CSP is only `frame-ancestors 'self';` — no `default-src`, no `object-src 'none'`, no script/resource restrictions. The page accepts user input via a textarea, so stored/reflected XSS is a real risk.
- **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';
    upgrade-insecure-requests;
  ```

  Generate the nonce per request server-side and add it to every inline `<script>`.

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

- **Impact:** WCAG 1.4.3 (AA), axe serious violation
- **Problem:** axe reports a serious `color-contrast` violation on `.menu-item-116 > .navigation__description`, `.menu-item-74 > .navigation__description` and `.menu-item-75 > .navigation__description`; one further node was inconclusive.
- **Solution:** Raise the text/background contrast of `.navigation__description` to at least 4.5:1 (3:1 if the text is ≥24 px or ≥19 px bold):

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

  - Check the one node axe marked *incomplete* manually (likely a gradient or alpha background).

Priority 2: Important

Essential for compliance, user reach, and search visibility.

2A. Fix color contrast on navigation descriptions `Accessibility`

- **Impact:** WCAG 1.4.3 contrast, axe serious violation
- **Problem:** axe reports 1 serious `color-contrast` violation on `.menu-item-75 > .navigation__description`, plus 1 node it could not determine.
- **Solution:**
  - Raise the text/background contrast for `.navigation__description` to at least 4.5:1 for normal-size text (3:1 only if ≥18.66 px bold or ≥24 px).

- Re-test the element axe marked *incomplete* manually, since it likely uses alpha or a gradient.

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

- **Impact:** XSS defense-in-depth
- **Problem:** CSP is only `frame-ancestors 'self';` — the security basics advanced tier fails it for missing `default-src` and `object-src 'none'`, leaving scripts and resources unrestricted.
- **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 a login or user-generated content, move to a nonce-based policy with `'strict-dynamic'` rather than a flat allowlist.

2C. Replace vague "read more" link text `SEO`

- **Impact:** `link-text` SEO 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.
- **Solution:**
  - Rewrite each link to describe its destination, e.g. `<a href="/case-study-x">Read the X case study</a>`.
  - If the visible text must stay short, add `aria-label="Read more about X"`.

2D. Eliminate forced synchronous reflow `Performance`

- **Impact:** INP, main-thread layout cost
- **Problem:** PSI flags `forced-reflow-insight` at score 0.00 with high priority — layout is read after style writes during load.
- **Solution:**
  - Batch DOM reads (`offsetWidth`, `getBoundingClientRect`) before writes; never interleave them in a loop.
  - Cache measured values and apply style changes inside `requestAnimationFrame`.
  - Re-run Lighthouse after the fix to confirm the insight clears.

2E. Add explicit dimensions to the 5 unsized images `Best Practices`

- **Impact:** CLS (desktop currently 0.084)

- **Problem:** 5 of 30 images have no `width` / `height` attributes, which lets the browser reserve no space before load.
- **Solution:**
  - Add intrinsic `width` / `height` to each `<img>`.
  - For responsive images, add a CSS `aspect-ratio` so the box is reserved before the file loads.

2F. Add Cross-Origin-Opener-Policy and Cross-Origin-Resource-Policy `Security`

- **Impact:** Cross-window isolation, cross-origin read protection
- **Problem:** Both COOP and CORP are missing and both are flagged as fails in the security basics advanced tier.
- **Solution:**

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

2G. Block WordPress user enumeration `Security`

- **Impact:** Brute-force / credential-stuffing exposure
- **Problem:** Security basics reports "WordPress usernames can be enumerated" (fail) and the login form is served on the default `/wp-login.php` path (warn).
- **Solution:**
  - Block `?author=N` enumeration and REST user endpoints at the server:

```
RewriteCond %{QUERY_STRING} author=\d
RewriteRule ^ - [R=404,L]
```

  - Disable the `/wp-json/wp/v2/users` route for unauthenticated requests.
  - Move or protect the login path (custom login slug, or IP allowlist / basic auth in front of `wp-login.php`).

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

- **Impact:** WCAG 1.3.1 / 4.1.2 form labeling
- **Problem:** The HTML inventory shows a `textarea` in the contact form with no associated label (the other text inputs and one textarea are labeled).
- **Solution:** Add a visible `<label for="...">` or, if the field is intentionally hidden from sight, an `aria-label`:

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

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

- **Impact:** Supply-chain tampering risk
- **Problem:** 3 of 4 cross-origin scripts lack an `integrity` attribute — including the jsdelivr-hosted iframemanager and cookieconsent bundles.
- **Solution:** Pin 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.

2J. Block WordPress user enumeration and move the login path `Security`

- **Impact:** Attack surface, credential-stuffing reconnaissance
- **Problem:** Security basics reports WordPress usernames can be enumerated and the login form is served on the default `/wp-login.php` path.
- **Solution:**
  - Block `?author=N` enumeration at the server/WAF level and disable the REST users endpoint for anonymous requests.
  - Move the login form behind a custom path (e.g. a plugin or nginx `location` rewrite) and add rate limiting + 2FA.

2K. Eliminate console errors and the failing reCAPTCHA request `Best Practices`

- **Impact:** Lighthouse `errors-in-console`, user trust
- **Problem:** 5 console events were captured, including two `requestStorageAccess: Permission denied` errors, a CORS-blocked `styles__ltr.css` request (`net::ERR_FAILED`), and a failed preload asset — Lighthouse's `errors-in-console` audit fails.
- **Solution:**
  - Fix the reCAPTCHA stylesheet load failure (CORS / `Access-Control-Allow-Origin` on the gstatic asset, or upgrade the reCAPTCHA integration).
  - Investigate the `requestStorageAccess` denials — usually caused by third-party cookie restrictions in the embedded reCAPTCHA iframe.

- Re-run the runtime capture after the fix to confirm zero console errors.

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

- **Impact:** Rich results eligibility, mobile usability
- **Problem:** Lighthouse's modeled `structuredData` and `tapTargets` audits both fail; the single JSON-LD block is reported with type "Unknown".
- **Solution:**
  - Replace the unrecognized JSON-LD block with a valid schema.org type (e.g. `Organization` + `ContactPage` for this URL) and validate in the Rich Results Test.
  - Increase tap target sizes to at least 44×44 px with adequate spacing, especially in the footer and navigation link lists.

2M. Remove render-blocking resources and pull LCP under 2.5 s on mobile `Performance`

- **Impact:** LCP, FCP, Speed Index
- **Problem:** PSI mobile LCP is 2.9 s and FCP 1.95 s, with `render-blocking-insight` estimated at 650 ms of savings and Speed Index at 3.25 s.
- **Solution:**
  - Inline critical above-the-fold CSS and load the 3 external stylesheets asynchronously.
  - Preload the LCP element (font or hero asset) with `<link rel="preload" as="font" crossorigin>`.
  - Subset the 3 font files (105.3 KB, the largest resource type) to the weights actually used, or self-host with `font-display: swap`.

2N. Fix document caching (`cache-control: max-age=0` **)** `Performance`

- **Impact:** TTFB, repeat-visit LCP
- **Problem:** The document response sends `cache-control: max-age=0` despite WP Rocket being active, so every navigation revalidates a 389 KB decoded HTML document.
- **Solution:**
  - Confirm WP Rocket is actually serving cached HTML for this URL (check the `x-cache` / `wp-rocket` comment markers on a cold vs. warm request).
  - Serve HTML with a short TTL plus `stale-while-revalidate`, and long-lived immutable caching for hashed theme assets:

```
<FilesMatch "\.(js|css|woff2)$">
  Header set Cache-Control "public, max-age=31536000, immutable"
</FilesMatch>
```

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

- **Impact:** Screen-reader navigation, document outline
- **Problem:** The page jumps from `h1` ("Real Estate") straight to `h3` ("Real estate digital solutions"), flagged by axe (`heading-order`), W3C (line 457) and PSI's `heading-order` audit (score 0).
- **Solution:**
  - Change the "Real estate digital solutions" heading to `<h2>`, or insert an `<h2>` section heading before it.
  - Re-check the full outline: the page currently has h1 ×1, h2 ×3, h3 ×8 with no h4–h6, so the h3 case-study titles should sit under an h2.

2P. Fix heading hierarchy skip (h1 → h3) `Accessibility`

- **Impact:** Screen-reader document outline, PSI `heading-order` (weight 3), W3C validity
- **Problem:** The page jumps from the h1 "Management & Manufacturing" straight to an h3 (`.hero__description > h3`); axe flags `heading-order` as moderate, PSI's `heading-order` audit scores 0.00, and W3C reports the same skip as an error at line 457.
- **Solution:**
  - Change the hero subheading from `<h3>` to `<h2>`, or insert an `<h2>` between the h1 and the following h3s.
  - Re-check the full outline afterwards: the page currently has h1 ×1, h2 ×4, h3 ×13 with no h4–h6, so several h3s under "Index" may belong at h4.

2Q. Eliminate render-blocking resources and trim unused CSS/JS `Performance`

- **Impact:** FCP (1.95 s mobile), Speed Index (2.02 s), render-blocking insight (est. 740 ms)
- **Problem:** PSI flags `render-blocking-insight` as high with an estimated 740 ms saving, plus 12 KiB unused CSS, 29 KB unused JavaScript and 11 KiB legacy JavaScript; mobile FCP is 1.95 s versus 485 ms on desktop.
- **Solution:**
  - Inline critical above-the-fold CSS and defer the 3 external stylesheets.
  - Remove unused CSS rules (12 KiB est.) — WP Rocket's "Remove Unused CSS" option can do this.

- Drop the legacy JS bundle / jQuery Migrate if no plugin depends on it (11 KiB est.).
- Review the `network-dependency-tree-insight` finding: flatten the critical request chain so the LCP image and fonts are not queued behind scripts.

2R. Block WordPress username enumeration `Security`

- **Impact:** Brute-force / credential-stuffing exposure
- **Problem:** Security basics reports "WordPress usernames can be enumerated" as a fail, and the login form is still served on the default `/wp-login.php` path (warn).
- **Solution:**
  - Block `?author=N` enumeration and REST user endpoints at the server or via a security plugin:

```
RewriteCond %{QUERY_STRING} author=\d
RewriteRule ^ - [F]
```

  - Restrict `/wp-json/wp/v2/users` to authenticated requests.
  - Move or protect `/wp-login.php` (custom path, HTTP auth or IP allowlist).

Priority 3: Best Practice

Recommended for long-term maintainability.

3A. Trim unused CSS and legacy JavaScript `Performance`

- **Impact:** Render-blocking CSS, transfer size
- **Problem:** PSI estimates 11 KiB savings from `unused-css-rules` and 11 KiB from `legacy-javascript-insight`; jQuery and jquery-migrate are both loaded.
- **Solution:**
  - Remove `jquery-migrate` if no legacy plugin depends on it.
  - Drop unused CSS rules (or split per-template stylesheets).
  - Re-test with the Coverage panel to confirm the savings.

3B. Add HSTS preload, SRI, and reduce server disclosure `Security`

- **Impact:** Transport hardening, supply-chain integrity
- **Problem:** HSTS lacks the `preload` directive, 2 of 2 cross-origin jsDelivr scripts lack `integrity`, and `Server: Apache` is disclosed.
- **Solution:**
  - Extend HSTS: `max-age=31536000; includeSubDomains; preload`, then submit at hstspreload.org.

- Add `integrity` + `crossorigin` to the jsDelivr `<script>` tags.
- Set `ServerTokens Prod` / `ServerSignature Off` in Apache.

3C. Allow browser caching of the HTML document `Performance`

- **Impact:** Repeat-visit TTFB, back/forward navigation
- **Problem:** The document response is served with `cache-control: max-age=0` and an `Expires` equal to the request time, so the HTML is re-fetched on every visit.
- **Solution:**
  - Set a short but non-zero document TTL, e.g. `Cache-Control: public, max-age=600, stale-while-revalidate=60`.
  - Keep WP Rocket's page cache in front so the origin is not hit on each request.

3D. Declare a recognized structured-data type and enlarge tap targets `SEO`

- **Impact:** Rich results eligibility, mobile usability
- **Problem:** The modeled `structuredData` and `tapTargets` audits fail, and the single JSON-LD block is typed `Unknown`.
- **Solution:**
  - Replace the generic JSON-LD with a recognized schema.org type (`Organization`, `WebSite`, `Service`).
  - Ensure interactive targets are at least 24×24 px with adequate spacing (48×48 px recommended).

3E. 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, UGC or commerce, so real XSS impact is low and this is calibrated to P3.
- **Solution:** Add the missing directives at minimum:

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

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

3F. Add HSTS preload, COOP, CORP and hide the Server header `Security`

- **Impact:** Transport hardening, origin isolation, info disclosure

- **Problem:** HSTS lacks the `preload` directive, `Cross-Origin-Opener-Policy` and `Cross-Origin-Resource-Policy` are missing, and the `Server: Apache` header discloses technology.
- **Solution:**

```
Header always set Strict-Transport-Security "max-age=63072000;
includeSubDomains; preload"
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"
ServerTokens Prod
ServerSignature Off
```

  Submit the domain at hstspreload.org once the header is live.

3G. Add Subresource Integrity to jsDelivr scripts `Security`

- **Impact:** Third-party script tampering
- **Problem:** 2 of 2 cross-origin scripts (cookieconsent and iframemanager from cdn.jsdelivr.net) lack an `integrity` attribute.
- **Solution:** Pin 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>
```

  Generate the hash from the exact pinned file and update it whenever the version changes.

3H. Reduce legacy JavaScript and font payload `Performance`

- **Impact:** Main-thread work, transfer size
- **Problem:** PSI flags `legacy-javascript-insight` with ~11 KiB of estimated savings, and 3 font files account for 105.3 KB of the 244.7 KB total page weight.
- **Solution:**
  - Drop `jquery-migrate.min.js` if no plugin depends on it.
  - Set a modern browserslist target so the build stops shipping ES5 transpilation and polyfills.
  - Subset fonts to the used glyph ranges and serve WOFF2 only; consider `font-display: swap`.

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

- **Impact:** Rich results eligibility, link purpose
- **Problem:** PSI reports failing `structuredData` and `tapTargets` audits, the single JSON-LD block has type "Unknown", and 10 link texts repeat verbatim (e.g. "home" ×2, "contact" ×2).
- **Solution:**
  - Replace the unrecognized JSON-LD with a valid `@type` (e.g. `WebPage` / `Organization`) and validate in the Rich Results Test.
  - Disambiguate repeated nav links with `aria-label` or visually hidden text, e.g. `<a href="/contact/"><span class="sr-only">Contact us</span>Contact</a>`.
  - Increase tap target size to at least 44×44 px.

3J. Fix the two W3C validation errors `Best Practices`

- **Impact:** HTML conformance
- **Problem:** W3C reports 2 errors: hidden inputs carry `autocomplete='off'`, which is invalid on `type="hidden"` (first at line 885, `gform_hidden`).
- **Solution:** Remove `autocomplete` from hidden Gravity Forms inputs, or filter it out:

```
add_filter( 'gform_field_content', function( $content, $field ) {
    if ( 'hidden' === $field->type ) {
        $content = str_replace( " autocomplete='off'", '', $content
);
    }
    return $content;
}, 10, 2 );
```

3K. Add COOP/CORP, HSTS preload, and hide the Server header `Security`

- **Impact:** Origin isolation, HSTS preload eligibility, fingerprinting
- **Problem:** Cross-Origin-Opener-Policy and Cross-Origin-Resource-Policy are missing, HSTS lacks the `preload` directive, and the response discloses `Server: Apache`.
- **Solution:**

```
Header always set Cross-Origin-Opener-Policy "same-origin"
Header always set Cross-Origin-Resource-Policy "same-origin"
Header always set Strict-Transport-Security "max-age=63072000;
includeSubDomains; preload"
Header unset Server
```

  Then submit the domain at hstspreload.org.

3L. Set a real browser cache lifetime on the document `Performance`

- **Impact:** Repeat-visit TTFB, LCP
- **Problem:** The document response sends `cache-control: max-age=0` with an `Expires` equal to the request time, so repeat visitors revalidate the HTML every time despite WP Rocket being active.
- **Solution:**
  - Configure WP Rocket (or the server) to send a short but non-zero HTML cache lifetime, e.g. `Cache-Control: public, max-age=600, s-maxage=3600`.
  - Keep `Vary: Accept-Encoding` and add `ETag` / `Last-Modified` so conditional requests work.

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

- **Impact:** WCAG 4.1.2, screen-reader output
- **Problem:** axe reports 1 minor `presentation-role-conflict` violation on `iframe[title="reCAPTCHA"]`, and could not determine contrast for 3 nodes.
- **Solution:**
  - Remove `role="presentation"` / `role="none"` from the reCAPTCHA iframe wrapper, or stop applying it to a focusable element.
  - Manually verify the 3 unresolved color-contrast nodes with a contrast checker (axe skips gradient/alpha backgrounds).

3N. Disambiguate repeated link text `SEO`

- **Impact:** Anchor-text quality, screen-reader navigation
- **Problem:** The page repeats identical anchor text — "info@playandnope.com" ×3, "home" ×2, "work" ×2, "contact" ×2, and "play and nope alliance logo" ×2.
- **Solution:**
  - Add `aria-label` or visually-hidden context to repeated links, e.g. `<a href="/work/" aria-label="View our work portfolio">work</a>`.
  - Give the logo link an accessible name of the site rather than "play and nope alliance logo".

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

- **Impact:** XSS defense-in-depth
- **Problem:** The CSP only sets `frame-ancestors 'self'` — `default-src` is missing and `object-src` is not `'none'`, which is the failing advanced check.

Site signals show no auth, payments, user content or commerce, so this is P3 rather than P1.

- **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 a login or user content, move to a nonce + `'strict-dynamic'` policy rather than a flat allowlist.

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

- **Impact:** Transport hardening, cross-origin isolation, supply-chain 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 (jsdelivr) lack `integrity` attributes.
- **Solution:**

```
Header always set Strict-Transport-Security "max-age=31536000;
includeSubDomains; preload"
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"
```

  - Add `integrity` + `crossorigin` to the two `cdn.jsdelivr.net` scripts (iframemanager, cookieconsent).
  - Submit the domain at hstspreload.org once the preload directive is live.

3Q. Trim legacy and unused JavaScript `Performance`

- **Impact:** Main-thread work, transfer size
- **Problem:** PSI reports 30 KB of unused JavaScript on the page and `legacy-javascript-insight` with an estimated 11 KiB saving; 8 script requests total 100.3 KB.
- **Solution:**
  - Drop the `jquery-migrate` script if no plugin depends on it.
  - Serve modern-only bundles (`type="module"`) and remove legacy polyfill builds.
  - Defer or conditionally load the WP Rocket beacon until after first interaction.

3R. Add valid structured data and fix tap targets `SEO`

- **Impact:** Rich results eligibility, mobile usability

- **Problem:** PSI's modeled audits fail on `structuredData` and `tapTargets`, and the single JSON-LD block is reported with type "Unknown".
- **Solution:**
  - Replace the untyped JSON-LD block with a concrete `Organization` / `ProfessionalService` schema including `name`, `url`, `logo`, `sameAs` and `contactPoint`.
  - Validate with the Rich Results Test.
  - Increase mobile tap-target size to at least 44×44 px for the navigation and footer links.

3S. Reduce technology disclosure and duplicate link text `Best Practices`

- **Impact:** Fingerprinting surface, screen-reader link context
- **Problem:** The `Server: Apache` header discloses the stack, and 10 link texts repeat verbatim (e.g. "home" ×2, "work" ×2, "contact" ×2), which axe/W3C cannot disambiguate.
- **Solution:**
  - Suppress the server banner: `ServerTokens Prod` and `ServerSignature Off`.
  - Give duplicated nav links distinct accessible names via `aria-label` or visually hidden text, or mark the duplicate set `aria-hidden="true"` if it is a mobile-only clone of the desktop nav.

3T. Complete remaining header hardening (HSTS preload, COOP, CORP, SRI, server banner) `Security`

- **Impact:** Transport security, cross-origin isolation, supply-chain integrity
- **Problem:** HSTS lacks the `preload` directive, `Cross-Origin-Opener-Policy` and `Cross-Origin-Resource-Policy` are missing, 2 of 2 cross-origin jsDelivr scripts lack `integrity`, and the `Server: Apache` header discloses technology.
- **Solution:**

```
Header always set Strict-Transport-Security "max-age=63072000;
includeSubDomains; preload"
Header always set Cross-Origin-Opener-Policy "same-origin"
Header always set Cross-Origin-Resource-Policy "same-origin"
Header unset Server
```

  - Add `integrity` + `crossorigin` to the two `cdn.jsdelivr.net` scripts (cookieconsent, iframemanager), or self-host them.
  - Submit the domain at hstspreload.org once the header is live.

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

- **Impact:** Rich-result eligibility, mobile usability
- **Problem:** PSI's modeled audits `structuredData` and `tapTargets` both fail, and the single JSON-LD block is typed as "Unknown" so no recognized schema is being emitted.
- **Solution:**
  - Replace the unrecognized JSON-LD with a valid `Organization` / `Service` / `WebPage` graph and validate in the Rich Results Test.
  - Increase tap target size to at least 44×44 px for small nav and footer links.

3V. Fix invalid `</br>` end tags and document caching `Best Practices`

- **Impact:** W3C validity, repeat-visit performance
- **Problem:** W3C reports 3 errors, two of which are stray `End tag "br"` at line 489; the document response also sends `cache-control: max-age=0`, forcing revalidation on every visit.
- **Solution:**
  - Replace `</br>` with `<br>` (or `<br />`) in the template at line 489.
  - Give the HTML a short shared-cache TTL so repeat visits skip the round trip:

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