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

Website: https://playandnope.com/
Date: 12.10.2026
Audit Coverage: 96% — PageSpeed Insights (desktop): PSI request timed out after 120000ms; PageSpeed Insights (desktop): PSI HTTP 500; PageSpeed Insights: mobile: PSI request timed out after 120000ms; desktop: PSI HTTP 500
Confidence: low

Pages Audited (10 of 10):

- 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
- https://playandnope.com/digiagentuur-klientide-tagasiside
- https://playandnope.com/design-service
- https://playandnope.com/digital-product-development-services
- https://playandnope.com/digital-agency-feedback
- https://playandnope.com/scalable-e-commerce-solutions

Summary of results

Overall Score: 72 / 100
Status: □ □ **Needs Improvement**

Site overall 72 is the mean of 9 pages. Scores range 48 (https://playandnope.com/contact) → 88 (https://playandnope.com/scalable-e-commerce-solutions). Weakest page: PSI mobile Performance is 34 with catastrophic lab metrics — TBT 28.97 s, LCP 12.7 s, Speed Index 11.35 s and TTI 43.8 s — while Accessibility 99, Best Practices 96 and SEO 100 are all strong, so the score is dragged down almost entirely by main-thread collapse. The long-task trace points at first-party theme JS (core.js 784 ms, jquery.min.js 696 ms, global.min.js six tasks of 297–353 ms) plus 1.42 MB of reCAPTCHA from gstatic.com, where recaptcha__en.js is the slowest request at 3.36 s and three copies waste ~173 KB each. Desktop PSI errored (HTTP

500) and mobile data was duplicated for both strategies, so the mobile/desktop delta is unknown and confidence is medium. Security basics PASS, but the CSP is `frame-ancestors 'self';` only (no default-src, no object-src 'none'), HSTS lacks preload, COOP/CORP are missing and 3 of 4 cross-origin scripts lack SRI — with a textarea form present, XSS defense-in-depth is worth P1 attention. W3C reports 2 errors (hidden input with autocomplete) and axe only 1 minor violation, so markup and accessibility are not the drag; the document also ships `cache-control: max-age=0`, forcing revalidation on every navigation.

Per-page scores

 Poor · https://playandnope.com/

Score	Performance	Accessibility	Best Practices	SEO	Security
50	34	100	100	92	PASS

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

Score	Performance	Accessibility	Best Practices	SEO	Security
88	95	100	100	100	PASS

 Poor · https://playandnope.com/contact

Score	Performance	Accessibility	Best Practices	SEO	Security
48	34	99	96	100	PASS

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

Score	Performance	Accessibility	Best Practices	SEO	Security
64	54	98	100	100	PASS

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

Score	Performance	Accessibility	Best Practices	SEO	Security
—	—	—	—	—	PASS

 Needs Improvement · https://playandnope.com/digiagentuur-klientide-tagasiside

Score	Performance	Accessibility	Best Practices	SEO	Security
83	87	100	100	100	PASS

 Needs Improvement · https://playandnope.com/design-service

Score	Performance	Accessibility	Best Practices	SEO	Security
71	60	98	100	100	PASS

 Needs Improvement · https://playandnope.com/digital-product-development-services

Score	Performance	Accessibility	Best Practices	SEO	Security
68	60	98	100	100	PASS

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

Score	Performance	Accessibility	Best Practices	SEO	Security
88	95	100	100	100	PASS

 Needs Improvement · https://playandnope.com/scalable-e-commerce-solutions

Score	Performance	Accessibility	Best Practices	SEO	Security
88	94	98	100	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/	34 / —	5.53 s / —	0.000 / —
https://playandnope.com/privacy-policy	**95** / 97	**2.29 s** / 596 ms	0.085 / **0.093**
https://playandnope.com/contact	34 / —	12.67 s / —	0.057 / —

URL	Performance (M / D)	LCP (M / D)	CLS (M / D)
https://playandnope.com/full-stack-digital-agency	54 / —	3.34 s / —	0.000 / —
https://playandnope.com/digiagentuur-klientide-tagasiside	**87** / 95	**3.79 s** / 617 ms	0.040 / **0.129**
https://playandnope.com/design-service	**60** / 75	**4.06 s** / 542 ms	1.000 / **1.083**
https://playandnope.com/digital-product-development-services	60 / —	2.38 s / —	0.000 / —
https://playandnope.com/digital-agency-feedback	**95** / 97	**2.50 s** / 562 ms	0.001 / **0.101**
https://playandnope.com/scalable-e-commerce-solutions	**94** / 98	**2.63 s** / 663 ms	0.000 / **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

Item	Status	Detail
		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 30 s Total Blocking Time from long JavaScript tasks `Performance`

- **Impact:** TBT, TTI, INP, Max Potential FID
- **Problem:** TBT is 30,000 ms with long tasks from jQuery (956 ms), core.js (719 ms) and repeated global.js tasks (300–370 ms); 92 KB of global.js is unused.
- **Solution:**
  - Split `global.min.js` and `core.min.js` into route-level chunks so only the code the page needs is parsed.
  - Audit jQuery usage — if the theme only uses it for a few widgets, replace with vanilla JS or drop it.
  - Tree-shake the 92 KB of unused code reported for `global.62444fa2566b44750ca1.min.js`.
  - Move non-critical work (analytics, cookie consent, iframe manager) behind `requestIdleCallback` or a user-interaction trigger.
  - Re-measure TBT after each change; target <200 ms.

1B. Fix LCP 5.0 s and FCP 4.14 s `Performance`

- **Impact:** LCP, FCP, Speed Index
- **Problem:** LCP is 5.0 s and FCP 4.14 s; the `lcp-breakdown-insight` and `network-dependency-tree-insight` audits both scored 0.00.
- **Solution:**
  - Identify the LCP element in DevTools Performance panel (the breakdown insight failed, so this must be done manually).

- If the LCP element is text, preload the webfont and add `font-display: swap`; the runtime shows 3 font files totalling 105.3 KB.
- If it is an image, add `<link rel="preload" as="image" fetchpriority="high">` for the hero.
- Flatten the critical request chain — the network-dependency-tree insight failed, so inspect the waterfall for serialized requests.
- Inline critical CSS (3 inline stylesheets, 9.6 KB) and defer the rest.

1C. Fix color-contrast on navigation menu descriptions and links `Accessibility`

- **Impact:** WCAG 2.1 AA 1.4.3, navigation readability
- **Problem:** axe reports 1 serious color-contrast violation on `.navigation__description` (menu items 14, 630, 116) and `.navigation__link[target="_self"]` (menu item 75); 9 further nodes are flagged as 'incomplete' because axe could not determine contrast.
- **Solution:** Raise the foreground/background contrast ratio to at least 4.5:1 for normal text and 3:1 for large text:

  ```
  .navigation__description { color: #4a4a4a; } /* was too light */
  .navigation__link { color: #1a1a1a; }
  ```

  Verify the 9 'incomplete' nodes manually (axe skips elements with alpha-transparency or gradients).

1D. Eliminate 28.97 s of main-thread blocking `Performance`

- **Impact:** TBT, TTI, INP, Max Potential FID
- **Problem:** TBT is 27,630 ms and TTI 43.8 s; long tasks come from core.js (784 ms), jquery.min.js (696 ms) and global.min.js (six tasks of 297–353 ms).
- **Solution:**
  - Code-split `global.min.js` and `core.min.js` per route; load only what the contact page needs.
  - Drop the jQuery dependency (696 ms task) in favour of vanilla DOM APIs, or at minimum defer it behind interaction.
  - Remove the 92 KB of unused JS reported in `global.62444fa2566b44750ca1.min.js`.
  - Audit the 44 scripts (16 defer, 2 async, 2 render-blocking) and consolidate bundles.

1E. Fix the 12.7 s LCP `Performance`

- **Impact:** LCP, Speed Index, FCP

- **Problem:** LCP is 12.7 s and Speed Index 11.35 s; `lcp-breakdown-insight` and `network-dependency-tree-insight` both score 0.00.
- **Solution:**
  - Preload the LCP element (`<link rel="preload" as="image" fetchpriority="high">` or font preload).
  - Inline critical CSS and remove the 2 render-blocking scripts.
  - Ensure the hero renders without waiting on JS execution — the current LCP is gated behind the 28.97 s main-thread queue.

1F. Load reCAPTCHA on demand instead of at page load `Performance`

- **Impact:** TBT, LCP, third-party bytes, page weight
- **Problem:** gstatic.com serves 1.42 MB across 7 requests; `recaptcha__en.js` is the slowest request at 3.36 s and three copies waste ~173 KB each.
- **Solution:**
  - Use `render=explicit` and only call `grecaptcha.render()` when the user focuses the contact form.
  - Show a click-to-load placeholder instead of the invisible badge on initial paint.
  - Consider a lighter challenge (hCaptcha, Turnstile) or server-side spam filtering to remove the third-party entirely.

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

- **Impact:** XSS defense-in-depth
- **Problem:** CSP is `frame-ancestors 'self';` only — no `default-src`, no `object-src 'none'`, no script/resource restrictions; the page contains a textarea form (hasUserContent = yes).
- **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';
  ```

  Generate the nonce per request and propagate it to the WordPress/Gravity Forms script tags.

1H. Break up long tasks in global.min.js to cut TBT `Performance`

- **Impact:** TBT, TTI, Max Potential FID, INP
- **Problem:** TBT is 17.36 s (Lighthouse score 0.00, weight 30) with 10 long tasks up to 468 ms in global.62444fa2566b44750ca1.min.js, pushing TTI to 45.3 s and Max Potential FID to 470 ms.

- **Solution:**
  - Split `global.min.js` into route-level chunks and load only what the page needs.
  - Defer non-critical init with `requestIdleCallback` / `setTimeout` after first paint.
  - Audit the 92 KB of unused JS reported by Lighthouse and drop dead code.
  - Consider `scheduler.yield()` or `await new Promise(r => setTimeout(r))` between independent init blocks.

1I. Shorten the critical request chain (Speed Index 6.47 s, 640 ms document latency) `Performance`

- **Impact:** Speed Index, FCP, LCP
- **Problem:** Speed Index is 6.47 s (score 0.45) and document-latency-insight estimates 640 ms of savings; FCP is 2.0 s.
- **Solution:**
  - Inline critical CSS and defer the 3 external stylesheets.
  - Preload the LCP image and the primary font.
  - Reduce the 195 KB HTML document (large inline payload) and trim the 9.6 KB of inline styles.
  - Add `<link rel="preconnect">` for `cdn.jsdelivr.net` (currently 0 preconnects, 6 requests to jsdelivr).

1J. Reduce mobile LCP (3.8 s) `Performance`

- **Impact:** LCP, FCP, Speed Index
- **Problem:** Mobile LCP is 3.8 s vs 0.6 s on desktop; the network-dependency-tree insight is flagged high and document-latency-insight estimates 610 ms of savings.
- **Solution:**
  - Preload the LCP image and any critical font:

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

  - Flatten the critical request chain (inline critical CSS, defer non-critical JS).
  - Serve the LCP asset from the same origin / CDN edge to cut the extra hop.

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

- **Impact:** WCAG 1.4.3 (contrast), 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`.
- **Solution:**
  - Darken the `.navigation__description` text color to reach ≥4.5:1 against its background.
  - Verify with DevTools contrast checker; axe also flagged 8 incomplete contrast nodes (likely gradients/alpha) that need manual review.

1L. Eliminate the 1.000 CLS caused by the hero background `Performance`

- **Impact:** CLS, mobile Performance score
- **Problem:** PSI reports CLS 1.000 on mobile (1.083 desktop) with the sole culprit being div.hero > div.hero__bg (shift 1.000) — 4× the 'heavy penalty' threshold.
- **Solution:** Reserve space for the hero background before it paints:
  - Give the hero container a fixed `aspect-ratio` or explicit `min-height` so the background cannot push content.
  - If the background is injected by JS, render a placeholder with the same dimensions server-side.

```
.hero { aspect-ratio: 16 / 9; }
.hero__bg { position: absolute; inset: 0; }
```

1M. Reduce mobile LCP from 4.1 s `Performance`

- **Impact:** LCP, FCP, Speed Index
- **Problem:** Mobile LCP is 4.1 s vs 0.5 s on desktop; PSI's document-latency-insight estimates 640 ms of savings and FCP is 2.01 s.
- **Solution:**
  - Preload the LCP image and set `fetchpriority="high"` on it.
  - Inline critical CSS for above-the-fold content.
  - Defer or remove non-critical scripts (global.min.js is 111 KB unused).

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

1N. Eliminate 24.86 s of Total Blocking Time from theme JavaScript `Performance`

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

- **Problem:** PSI reports TBT 24,540 ms (audit value 29,540 ms) and TTI 44.4 s, with long tasks in jquery.f5f8c1b60d5ba64e00fb.min.js (1.03 s), core.c872dceb075db34864df.min.js (829 ms) and seven ~400 ms tasks in global.62444fa2566b44750ca1.min.js.
- **Solution:** The page renders quickly (LCP 2.6 s) but the main thread is blocked for tens of seconds. Profile and split the theme bundle:
  - Open DevTools Performance, record a load, and identify which functions inside `global.min.js` run repeatedly (~400 ms × 7 suggests a loop or repeated init).
  - Defer non-critical init until after `load` or `requestIdleCallback`.
  - Drop jQuery Migrate (`jquery-migrate.min.js` is loaded) if the theme no longer needs it.
  - Consider replacing jQuery-dependent widgets with vanilla JS or lazy-loading them on interaction.

1O. Remove 92 KB of unused JavaScript from global.min.js `Performance`

- **Impact:** TBT, Speed Index, page weight
- **Problem:** PSI flags 92 KB wasted in `global.62444fa2566b44750ca1.min.js`, and the same file is responsible for most of the long tasks.
- **Solution:** Run Lighthouse's coverage report and code-split `global.min.js`:
  - Move code paths only used on specific templates (e.g. sliders, modals, cookie banner) into separate chunks loaded on demand.
  - Tree-shake unused exports and drop polyfills for modern browsers.
  - Verify with `npx source-map-explorer` or the Coverage panel.

1P. Fix color-contrast on navigation links `Accessibility`

- **Impact:** WCAG 1.4.3 (AA), axe serious violation
- **Problem:** axe reports 1 serious color-contrast violation on `.menu-item-74 > .navigation__link` / `.navigation__description` and the same for `.menu-item-75`, plus 9 incomplete nodes it could not evaluate.
- **Solution:** Raise the nav link and description colors to ≥4.5:1 against their background:

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

Then re-run axe and manually check the 9 incomplete nodes (likely alpha/gradient backgrounds).

1Q. Fix document caching (cache-control: max-age=0) `Performance`

- **Impact:** Repeat-visit TTFB, LCP, FCP
- **Problem:** The document response returns `cache-control: max-age=0` with `expires` set to the request time, so browsers revalidate on every navigation despite WP Rocket being detected.
- **Solution:** Configure WP Rocket / the origin to emit a positive max-age for the HTML document, e.g.:

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

  Keep `max-age=0` only for logged-in or personalized responses.

Priority 2: Important

Essential for compliance, user reach, and search visibility.

2A. Fix forced reflow / layout thrashing `Performance`

- **Impact:** TBT, INP
- **Problem:** The `forced-reflow-insight` audit scored 0.00, indicating synchronous layout reads after DOM writes.
- **Solution:**
  - Batch DOM reads before writes; avoid reading `offsetHeight` / `getBoundingClientRect` inside loops that mutate the DOM.
  - Use `requestAnimationFrame` to schedule layout-dependent work.
  - Cache layout values instead of re-reading them per iteration.

2B. Replace vague repeated link text `SEO`

- **Impact:** SEO, link-text audit, screen-reader navigation
- **Problem:** The `link-text` SEO audit failed with 4 links; the inventory shows "read more" ×4 plus repeated "development", "design & innovation" and "technical maintenance" anchors.
- **Solution:**
  - Replace "read more" with descriptive text, e.g. "Read more about our development services".
  - Where the visible label must stay short, add `aria-label`:

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

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

- **Impact:** SEO, mobile usability, rich results
- **Problem:** The `tapTargets` and `structuredData` SEO audits both failed; the single JSON-LD block is typed "Unknown".
- **Solution:**
  - Enlarge interactive targets to at least 44×44 px with adequate spacing (WCAG 2.5.8).
  - Replace the untyped JSON-LD with a valid schema.org graph, e.g. `Organization` + `WebSite` + `Service` for an agency site:

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

2D. 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.
- **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 so they are covered by your own CSP and cache.

2E. Add explicit width/height to 5 images `Best Practices`

- **Impact:** CLS
- **Problem:** 5 of 30 images lack explicit width/height; CLS is currently 0.000 but the risk is latent.
- **Solution:**
  - Add `width` / `height` attributes to every `<img>`.
  - For responsive images, set `aspect-ratio` in CSS so the box is reserved before load:

```
.card img { aspect-ratio: 360 / 270; width: 100%; height: auto; }
```

2F. Add HSTS preload directive `Security`

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

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

2G. Reduce unused JavaScript in global.min.js `Performance`

- **Impact:** TBT, main-thread work, page weight
- **Problem:** `global.62444fa2566b44750ca1.min.js` ships 112 KB of unused JavaScript and produces a 96 ms long task on mobile.
- **Solution:**
  - Code-split the bundle so only the modules used on this page load.
  - Tree-shake and drop jQuery-dependent code where possible.
  - Keep `defer` on all theme scripts (already in place).

2H. Move 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' as a warn — the login form is served on `/wp-login.php`.
- **Solution:**
  - Rename the login URL (e.g. via a plugin or server rewrite).
  - Add rate limiting and 2FA on the login endpoint.
  - Keep `xmlrpc.php` blocked (already passing).

2I. Enable browser caching for the HTML document `Performance`

- **Impact:** repeat-visit LCP, TTFB
- **Problem:** The document response sets `cache-control: max-age=0`, so every navigation revalidates even though WP Rocket is detected.
- **Solution:**
  - Set a short but non-zero document TTL with revalidation, e.g. `Cache-Control: public, max-age=600, stale-while-revalidate=60`.

    - Verify WP Rocket's browser-cache rules are actually applied to the canonical URL.

2J. Add HSTS preload and COOP/CORP headers `Security`

- **Impact:** TLS downgrade protection, cross-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=31536000; includeSubDomains;
preload
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
```

  Then submit the domain at hstspreload.org.

2K. Resolve the reCAPTCHA console error `Best Practices`

- **Impact:** Best Practices score, form reliability
- **Problem:** `requestStorageAccess: Permission denied.` is logged from the reCAPTCHA anchor iframe, failing the `errors-in-console` audit.
- **Solution:**
    - Investigate whether the storage-access denial breaks the invisible reCAPTCHA challenge on Safari/Firefox.
    - If it does, switch to a challenge that does not depend on third-party storage, or self-host the widget.

2L. Label the unlabelled textarea `Accessibility`

- **Impact:** WCAG 1.3.1, 4.1.2
- **Problem:** Form 1 contains a `textarea` with no label (the 12 hidden inputs do not require labels).
- **Solution:**

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

  Or add `aria-label="Message"` if a visible label is not desired.

2M. Fix the presentation-role conflict on the reCAPTCHA iframe `Accessibility`

- **Impact:** WCAG 4.1.2
- **Problem:** axe reports `presentation-role-conflict` on `iframe[title="reCAPTCHA"]` — the only violation found (minor).

- **Solution:**
  - Remove `role="presentation"` / `aria-hidden="true"` from the reCAPTCHA iframe or its wrapper.
  - Keep the `title` attribute so the frame retains an accessible name.

2N. Disambiguate repeated vague link text `SEO`

- **Impact:** link purpose, crawlability
- **Problem:** 43 anchors include repeated vague text: "info@playandnope.com" ×3, "home" ×2, "work" ×2, "about" ×2, "contact" ×2, "business transformation" ×2 and others.
- **Solution:**
  - Add `aria-label` or visually hidden context to each repeated link, e.g. `<a href="/work" aria-label="View our work">work</a>`.
  - Ensure the surrounding heading or list item provides context for screen-reader users.

2O. Add valid structured data `SEO`

- **Impact:** rich results eligibility
- **Problem:** PSI's `structuredData` audit fails and the single JSON-LD block is typed "Unknown".
- **Solution:** Add an `Organization` / `LocalBusiness` block with `name`, `url`, `logo`, `contactPoint` and a `ContactPage` for this URL:

```
{"@context":"https://schema.org","@type":"Organization","name":"gotoAndPlay","url":"https://playandnope.com/","contactPoint":{"@type":"ContactPoint","contactType":"sales","email":"info@playandnope.com"}}
```

2P. Enlarge mobile tap targets `SEO`

- **Impact:** mobile usability
- **Problem:** PSI's `tapTargets` audit fails on mobile.
- **Solution:**
  - Ensure every interactive element is at least 44×44 px with adequate spacing.
  - Check the nav links, footer links and form controls at a 375 px viewport.

2Q. Serve modern image formats and right-size JPGs `Performance`

- **Impact:** Image bytes, LCP

- **Problem:** image-delivery-insight estimates 87 KiB of savings; browser runtime shows 8 images at 287.5 KB, with JPGs like img-10-393x440.jpg (34.0 KB) taking 648 ms each.
- **Solution:**
  - Convert the uploaded JPGs to WebP/AVIF with a `<picture>` fallback.
  - Ensure the served width matches the rendered width (the 393×440 and 440×294 variants suggest oversized delivery).
  - Keep the existing `srcset`, `width` / `height` and `loading="lazy"` attributes — they are already correct.

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

- **Impact:** WCAG 1.3.1, screen-reader navigation
- **Problem:** axe reports 1 moderate `heading-order` violation on `.hero__description > h3`, and W3C reports the same error at line 467: h3 follows h1, skipping a level.
- **Solution:**
  - Change the hero `<h3>Full-stack digital agency powered by curiosity</h3>` to `<h2>`, or insert an `<h2>` between it and the `<h1>Get to know us`.
  - Review the outline: `h2: People who make impossible possible` is immediately followed by `h2: Graphic & Brand Designer`, which reads as a job title rather than a section heading.

2S. Set a real Cache-Control policy on the HTML document `Performance`

- **Impact:** Repeat-visit TTFB, LCP
- **Problem:** The document response sets `cache-control: max-age=0` with `expires` equal to the response date, so every navigation revalidates despite WP Rocket being active.
- **Solution:**
  - Serve HTML with a short shared-cache TTL plus stale-while-revalidate, e.g. `Cache-Control: public, max-age=600, stale-while-revalidate=86400`.
  - Ensure WP Rocket page cache is warmed for the canonical URL so the first visitor does not pay the cold-start cost.

2T. Ship source maps for first-party JavaScript `Best Practices`

- **Impact:** Debuggability, error monitoring
- **Problem:** Lighthouse flags `valid-source-maps` (score 0.00): missing source maps for large first-party JavaScript such as global.62444fa2566b44750ca1.min.js.

- **Solution:**
  - Emit `.map` files alongside the minified bundles and reference them with `//# sourceMappingURL=`.
  - If maps must stay private, upload them to your error-tracking service instead of serving them publicly.

2U. Trim unused JavaScript in global.min.js `Performance`

- **Impact:** TBT, LCP, main-thread work
- **Problem:** 112 KB of unused JS in `global.62444fa2566b44750ca1.min.js` and an 86 ms long task from the same file; legacy-javascript-insight estimates 10 KiB of savings.
- **Solution:**
  - Audit the bundle with `npx source-map-explorer` and remove dead modules.
  - Split the bundle so only route-relevant code loads on this page.
  - Drop legacy polyfills via `browserslist` targeting modern browsers.

2V. Eliminate hero grid layout shift (desktop CLS 0.129) `Performance`

- **Impact:** CLS
- **Problem:** Desktop CLS is 0.129 (warning band); the shift source is `div.hero > div.hero__inner > div.grid > div.grid__col` (shift 0.040).
- **Solution:**
  - Reserve space for the hero grid with explicit `min-height` / `aspect-ratio`.
  - Avoid injecting content above the fold after load (fonts, cookie banner, iframe manager).
  - Set `font-display: optional` or preload the webfonts to prevent late text reflow.

2W. Fix failing tap-target sizes `Accessibility`

- **Impact:** WCAG 2.5.8 (target size), mobile usability
- **Problem:** PSI's modeled `tapTargets` audit fails on mobile, indicating interactive elements below the 44×44 px minimum.
- **Solution:**
  - Increase padding on nav links and icon buttons to at least 44×44 px.
  - Verify with Chrome DevTools' mobile emulation and Lighthouse's tap-targets audit.

2X. Remove 111 KB of unused JavaScript `Performance`

- **Impact:** TBT, LCP, main-thread work
- **Problem:** PSI flags 111 KB wasted in global.62444fa2566b44750ca1.min.js, which also produces a 141 ms long task.
- **Solution:**
  - Code-split the theme bundle so only the modules used on this page load.
  - Audit jQuery/jQuery-Migrate usage — both are loaded but may be unnecessary on a marketing page.
  - Enable source maps (PSI flags `valid-source-maps` as failing).

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

- **Impact:** Repeat-visit TTFB, LCP
- **Problem:** The document response sends `cache-control: max-age=0` with an `expires` in the past, so browsers revalidate on every visit despite WP Rocket being detected.
- **Solution:** Configure WP Rocket / server to send a positive `max-age` with `stale-while-revalidate` for HTML, e.g.:

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

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

- **Impact:** Screen-reader navigation, WCAG 1.3.1
- **Problem:** axe flags a moderate heading-order violation on `h3[data-path-to-node="1"]`, and W3C reports the same skip after the h1 "Design & Innovation".
- **Solution:** Change the first h3 ("UX/UI design services, brand design & product innovation") to an h2, or insert an h2 before it. Verify the full outline stays sequential (h1 ×1, h2 ×4, h3 ×26).

2[. Add sizes attribute to srcset images `Best Practices`

- **Impact:** HTML validity, responsive image selection
- **Problem:** W3C reports an error at line 507: a `<source>` with width descriptors in `srcset` is missing the required `sizes` attribute.
- **Solution:** Add a `sizes` attribute matching the rendered width, e.g.:

```
<source srcset="img-800.webp 800w, img-1600.webp 1600w"
        sizes="(max-width: 800px) 100vw, 800px" type="image/webp">
```

2. Convert JPEG portfolio images to WebP/AVIF `Performance`

- **Impact:** Page weight, LCP, Speed Index

- **Problem:** Runtime capture shows 8 image requests totalling 595.2 KB out of 833.9 KB total, all JPEG (e.g. `tccg-s-2-600x448.jpg` 59.2 KB, `ega-s-440x329.jpg` 30.5 KB), and no WebP/AVIF is served.
- **Solution:** Serve modern formats with a fallback:

  ```
  <picture>
    <source type="image/avif" srcset="img-440.avif 440w, img-880.avif
  880w">
    <source type="image/webp" srcset="img-440.webp 440w, img-880.webp
  880w">
    <img src="img-440.jpg" srcset="img-440.jpg 440w, img-880.jpg
  880w" alt="…" width="440" height="329" loading="lazy">
  </picture>
  ```

  WP Rocket / Imagify can generate these automatically.

2]. Fix heading hierarchy (h1 → h3 skip, 50 h3s) `Accessibility`

- **Impact:** Screen-reader navigation, WCAG 1.3.1 / 2.4.6
- **Problem:** The page has h1 ×1, h2 ×1, h3 ×50 with no h4s, and both axe (`heading-order`, moderate) and W3C (1 error, line 469) flag the h1→h3 skip after "Projects we've worked on".
- **Solution:** Restructure the outline:
  - Promote the first section heading to `<h2>` so the sequence is h1 → h2 → h3.
  - Use `<h2>` for major sections (services, projects, contact) and reserve `<h3>` for cards inside them.
  - Re-run axe and the W3C validator to confirm.

2^. Tighten the Content-Security-Policy `Security`

- **Impact:** XSS defense-in-depth
- **Problem:** CSP is `frame-ancestors 'self';` only — no `default-src`, no `object-src 'none'`, so scripts, styles and plugins are unrestricted.
- **Solution:** Add a nonce-based policy with `'strict-dynamic'`:

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

  Roll out in report-only mode first to catch breakage from the jsdelivr cookie-consent scripts.

2_. Add Subresource Integrity to jsdelivr scripts `Security`

- **Impact:** Supply-chain integrity

- **Problem:** Security basics flags 2 of 2 cross-origin scripts lacking an `integrity` attribute; both are loaded from `cdn.jsdelivr.net` (cookieconsent, iframemanager).
- **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 hashes with `openssl dgst -sha384 -binary file.js | openssl base64 -A`.

**2`. Fix failing SEO audits: tap targets and structured data**` SEO`

- **Impact:** Mobile usability, rich results eligibility
- **Problem:** PSI reports `tapTargets` and `structuredData` as failing modeled SEO audits; the JSON-LD block is present but its type is reported as Unknown.
- **Solution:**
  - Ensure interactive elements (nav links, buttons) are at least 48×48 px with adequate spacing on mobile.
  - Replace the generic JSON-LD with a specific `@type` (e.g. `Organization`, `WebSite`, `Service`) and validate at https://validator.schema.org/.

2a. Optimize font loading `Performance`

- **Impact:** FCP, LCP, page weight
- **Problem:** Fonts are the largest resource type at 105.3 KB across 3 files, and FCP is 2.26 s on mobile — the weakest CWV metric.
- **Solution:**
  - Subset fonts to the glyphs actually used.
  - Preload the primary font with `<link rel="preload" as="font" type="font/woff2" crossorigin>`.
  - Use `font-display: swap` and consider self-hosting to avoid the jsdelivr round-trip.

2b. Fix heading level skip (h1 → h3) `Accessibility`

- **Impact:** WCAG 1.3.1, screen-reader document outline
- **Problem:** The hero section jumps from h1 to h3 (`.hero__description > h3`), which axe flags as a moderate heading-order violation and W3C reports as the page's only error at line 468.

- **Solution:** Change the hero subheading to `<h2>` so the outline descends sequentially:

  ```
  <h1>E-commerce &amp;amp; Marketplace</h1>
  <h2>Scalable e-commerce solutions for global growth</h2>
  ```

  Audit the remaining h3s (13 total) to confirm each sits under an h2.

2c. Shorten the critical network dependency chain `Performance`

- **Impact:** LCP, FCP, document latency
- **Problem:** PSI flags `network-dependency-tree-insight` **(high)** and `document-latency-insight` with an estimated 540 ms savings; the browser runtime shows the document request taking 508 ms.
- **Solution:**
  - Preload the LCP image and critical fonts.
  - Add `<link rel="preconnect">` for `cdn.jsdelivr.net` (currently 0 preconnects despite 6 requests to that origin).
  - Reduce the serial chain of deferred scripts so the LCP element can paint sooner.

Priority 3: Best Practice

Recommended for long-term maintainability.

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

- **Impact:** XSS defense-in-depth
- **Problem:** CSP is only `frame-ancestors 'self';` — no `default-src`, no `object-src 'none'`, so scripts and resources are unrestricted. Site signals show no auth, payments, UGC or ecommerce, so this is hardening rather than an exposure.
- **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';
  ```

  Roll it out in report-only mode first and watch for violations.

3B. Add HSTS preload and cross-origin isolation headers `Security`

- **Impact:** Transport security, cross-origin isolation

- **Problem:** HSTS is `max-age=31536000; includeSubDomains` but lacks `preload`; COOP and CORP 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 once the preload directive is live.

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

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

3D. Manually verify color contrast on 19 undetermined nodes `Accessibility`

- **Impact:** WCAG 1.4.3 contrast
- **Problem:** axe reports 0 violations but could not determine contrast for 19 nodes and link-in-text-block for 1 node.
- **Solution:**
  - Check the 19 flagged nodes with a contrast checker, including any text over gradients or alpha backgrounds that axe skips.
  - Ensure in-text links are distinguishable by more than color alone (underline or weight).

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

- **Impact:** XSS defense-in-depth
- **Problem:** CSP is only `frame-ancestors 'self';` — no `default-src`, no `object-src 'none'`, so no script/resource restrictions are enforced. Site signals show no auth, payments, or user content, so this is P3 rather than P1.
- **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';
```

3F. 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; the security headers section rates them low priority.
- **Solution:**

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

3G. Optimize web font loading `Performance`

- **Impact:** Page weight, FCP
- **Problem:** Fonts are the largest resource type at 105.3 KB across 3 requests, and mobile FCP is 1.97 s (just above the 1.8 s good threshold).
- **Solution:**
  - Subset fonts to the glyphs actually used.
  - Preload the primary font file.
  - Use `font-display: swap` and prefer WOFF2.

3H. Eliminate the /privacy-policy → /privacy-policy/ redirect `Performance`

- **Impact:** Document latency, FCP
- **Problem:** `document-latency-insight` is flagged high with est. savings of 690 ms; the browser runtime shows a 502 ms document request to `/privacy-policy` before the 78 ms `/privacy-policy/` response.
- **Solution:** Link to the canonical URL directly:

```
<a href="https://playandnope.com/privacy-policy/">Privacy
Policy</a>
```

3I. Add structured data `SEO`

- **Impact:** Rich results eligibility
- **Problem:** The `structuredData` modeled audit is failing and the single JSON-LD block is typed 'Unknown'.
- **Solution:** Add Organization / WebSite schema:

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

3J. Ship source maps for first-party JavaScript `Best Practices`

- **Impact:** debuggability
- **Problem:** `valid-source-maps` fails — large first-party bundles (core, jquery, global) have no source maps.
- **Solution:** Emit `.map` files in the build and reference them with `//# sourceMappingURL=` ; exclude them from production delivery if you prefer, but keep them available for error reporting.

3K. Move the login off the default /wp-login.php path `Security`

- **Impact:** brute-force surface
- **Problem:** The WordPress login form is served on the default `/wp-login.php` path.
- **Solution:**
  - Rename the login URL (e.g. WPS Hide Login) or restrict it by IP / basic auth at the edge.
  - Add rate limiting and 2FA for all administrator accounts.

3L. Stop disclosing the server technology `Security`

- **Impact:** information disclosure
- **Problem:** The response header `server: Apache` discloses the web server software.
- **Solution:**

  ```
  ServerTokens Prod
  ServerSignature Off
  ```

  Or strip the `Server` header at the reverse proxy.

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

- **Impact:** HTML validity
- **Problem:** W3C reports 2 errors: `<input type='hidden' autocomplete='off' class='gform_hidden' …>` — hidden inputs must not carry `autocomplete="on"` or `"off"` .
- **Solution:** Remove the `autocomplete` attribute from Gravity Forms hidden inputs, or filter it out:

  ```
  add_filter( 'gform_field_content', function( $content ) {
      return preg_replace( '/\sautocomplete=[\'"](on|off)[\'"]/', '',
  ```

```
$content );
} );
```

3N. Manually verify contrast on the 23 unresolved nodes `Accessibility`

- **Impact:** WCAG 1.4.3
- **Problem:** axe could not determine color contrast for 23 nodes (alpha-transparency or gradients) and flagged 1 link that may rely on color alone.
- **Solution:**
  - Check the 23 nodes with a contrast checker against the actual rendered background.
  - Add a non-color affordance (underline, icon) to the flagged in-text link.

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

- **Impact:** Origin isolation, cross-origin data leaks
- **Problem:** COOP and CORP are both missing from the response headers; the site loads 6 requests from cdn.jsdelivr.net.
- **Solution:**

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

3P. Add the HSTS preload directive `Security`

- **Impact:** First-visit MITM protection
- **Problem:** HSTS is `max-age=31536000; includeSubDomains` but lacks `preload`, so the domain cannot be submitted to the preload list.
- **Solution:**
  - Append `preload` to the header: `Strict-Transport-Security: max-age=31536000; includeSubDomains; preload`.
  - Submit the domain at hstspreload.org once the header is live.

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

- **Impact:** Supply-chain tampering risk
- **Problem:** 2 of 2 cross-origin scripts (from cdn.jsdelivr.net) lack an `integrity` attribute.
- **Solution:**

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

```
/cookieconsent.umd.js"
        integrity="sha384-…" crossorigin="anonymous" defer>
</script>
```

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

3R. 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 or genericise the `Server` header (`ServerTokens Prod`, `ServerSignature Off`).
  - Move or alias the login form to a non-default path and rate-limit it.

3S. Fix failing structured-data and touch-target audits `SEO`

- **Impact:** Rich results, mobile usability
- **Problem:** PSI lists `structuredData` and `tapTargets` as failing modeled audits; the single JSON-LD block is reported with type `Unknown`.
- **Solution:**
  - Declare an explicit `@type` (e.g. `Organization` / `ProfessionalService`) in the JSON-LD block.
  - Ensure interactive elements meet the 44×44 px minimum touch-target size.

3T. Disambiguate repeated link text `SEO`

- **Impact:** Link purpose, screen-reader navigation
- **Problem:** The HTML inventory flags repeated vague link text: "work" ×2, "about" ×2, "contact" ×2, "home" ×2, "design & innovation" ×2, "development" ×2, "business transformation" ×2, "technical maintenance" ×2.
- **Solution:**
  - Add `aria-label` or visually hidden context to each duplicate link, e.g. `<a href="/work" aria-label="View our work">work</a>`.
  - Where the duplicates are nav vs. footer, differentiate with `aria-label="Primary"` / `aria-label="Footer"` on the surrounding `<nav>`.

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

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

- **Problem:** CSP is only `frame-ancestors 'self';` — no `default-src` and no `object-src 'none'`. Site signals show no auth, payments, or user content, so the XSS surface is low.
- **Solution:** Add a restrictive baseline:

  ```
  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-src.

3V. Add HSTS preload directive `Security`

- **Impact:** Transport security hardening
- **Problem:** HSTS is `max-age=31536000; includeSubDomains` but lacks `preload`.
- **Solution:**
  - Append `preload` to the header and submit the domain at hstspreload.org.

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

3W. Set COOP and CORP headers `Security`

- **Impact:** Cross-origin isolation
- **Problem:** Cross-Origin-Opener-Policy and Cross-Origin-Resource-Policy are both missing.
- **Solution:**

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

3X. Suppress the Server header `Best Practices`

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

  ```
  ServerTokens Prod
  ServerSignature Off
  ```

3Y. HSTS preload, server disclosure, and login path `Security`

- **Impact:** Transport hardening, information disclosure

- **Problem:** HSTS lacks the `preload` directive; the `Server: Apache` header discloses technology; the login form is served on the default `/wp-login.php` path.
- **Solution:**
  - Add `preload` to HSTS and submit to hstspreload.org.
  - Suppress the `Server` header (`ServerTokens Prod` / `Header unset Server`).
  - Move or restrict `/wp-login.php` (custom path, IP allowlist, or 2FA plugin).

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

- **Impact:** Brute-force / credential-stuffing surface
- **Problem:** Security basics warns that the login form is served on the default `/wp-login.php` path, which is the first target for automated credential attacks.
- **Solution:**
  - Rename the login URL with a plugin (e.g. WPS Hide Login) or restrict `/wp-login.php` by IP at the WAF.
  - Enforce strong passwords and 2FA for all admin accounts.

3[. Suppress the Server: Apache header `Best Practices`

- **Impact:** Technology disclosure
- **Problem:** The response discloses `Server: Apache`, and Security basics flags technology disclosure as a warn.
- **Solution:**

```
ServerTokens Prod
ServerSignature Off
```

  Or strip the header at the CDN/reverse proxy.

3. Disambiguate repeated link text and add preconnect `SEO`

- **Impact:** Link context, third-party connection setup
- **Problem:** The HTML inventory lists 10 repeated link texts (e.g. "work" ×2, "about" ×2, "contact" ×2, "development" ×2) and 0 preconnect hints despite 21 external links and 6 requests to cdn.jsdelivr.net.
- **Solution:**
  - Add `aria-label` or visually-hidden context to repeated nav links, e.g. `<a href="/work">Work<span class="sr-only"> — our portfolio</span></a>`.
  - Add a preconnect for the CDN:

```
<link rel="preconnect" href="https://cdn.jsdelivr.net" crossorigin>
```

3]. Strengthen Content-Security-Policy `Security`

- **Impact:** XSS defense-in-depth
- **Problem:** CSP is present but only sets `frame-ancestors 'self';` — missing `default-src` and `object-src 'none'`, so no script/resource restrictions apply. Site signals show no auth, payments, or user content, so real XSS risk is low.
- **Solution:** Add 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';
```

3^. Add HSTS preload and COOP/CORP headers `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=63072000; includeSubDomains;
preload
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
```

  Then submit the domain at hstspreload.org.

3_. Suppress server technology disclosure and move login off default path `Security`

- **Impact:** Attack-surface reduction
- **Problem:** The `Server: Apache` header is disclosed, and the login form is served on the default `/wp-login.php` path.
- **Solution:**
  - Hide the server banner: `ServerTokens Prod` and `ServerSignature Off` in Apache config.
  - Move the WP login to a custom slug (e.g. via a security plugin) and rate-limit it.

**3`. HSTS preload and move login off /wp-login.php**` Security`

- **Impact:** Transport hardening, brute-force surface

- **Problem:** HSTS is set with `max-age=31536000; includeSubDomains` but lacks `preload`, and Security basics warns the login form is served on the default `/wp-login.php` path.
- **Solution:**
  - Add `preload` to HSTS and submit the domain at hstspreload.org.
  - Move the login form to a custom path (e.g. via a WP security plugin) and rate-limit attempts.

3a. Cache the HTML document `Performance`

- **Impact:** TTFB on repeat visits, server load
- **Problem:** The document response sets `cache-control: max-age=0` with an `expires` equal to `date`, so the HTML is revalidated on every request despite WP Rocket being active.
- **Solution:** Configure WP Rocket (or the origin) to serve the HTML with a short positive `max-age` plus `s-maxage` for the CDN, e.g.:

  ```
  Cache-Control: public, max-age=600, s-maxage=3600, stale-while-revalidate=86400
  ```

  Keep the current fast TTFB (67 ms) as the baseline.

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

- **Impact:** Rich results eligibility, mobile usability
- **Problem:** PSI's modeled audits `structuredData` and `tapTargets` both fail, and the single JSON-LD block is reported with type `Unknown`.
- **Solution:**
  - Replace the generic JSON-LD with a typed schema (`Organization`, `Service`, or `BreadcrumbList`) validated in the Rich Results Test.
  - Ensure interactive elements meet the 44×44 px minimum touch target size.