Audit Report: Tere tulemast Paws N' Play veebilehele! — gotoAndPlay Demo WordPress Base

Website: https://demo.playandnope.com/
Date: 2026-07-12

Overall Score: 78 / 100
Status: **Needs Improvement**
Confidence: high
Audit Coverage: 100% — all sources returned data

Summary

Mobile performance is strong (90) but LCP (2.9s) falls in the warning zone due to the hero image incorrectly using lazy loading. Security posture is critically weak (20/100) because HTTP traffic does not redirect to HTTPS and HSTS is missing, despite the site being a brochure with no auth/payments. Accessibility is excellent (0 axe violations) but 10 W3C validation errors indicate code quality issues. The site is a pet care community/marketing site, which lowers CSP priority but not basic header requirements.

PageSpeed Insights — Mobile vs Desktop

*Lower is worse for Performance; higher is worse for LCP and CLS. Worse value is **bolded**.*

Strategy	Performance (M / D)	LCP (M / D)	CLS (M / D)
Mobile vs Desktop	**90** / 100	**2.86 s** / 727 ms	0.000 / **0.003**

Optimization Checklist

4 of 6 passing — 4 pass · 1 warn · 1 fail · 1 n/a

Item	Status	Detail
Page caching plugin / CDN active	**Pass**	Caching plugin detected (WP Rocket)
Images lazy-loaded	**Pass**	All non-hero raster images use loading="lazy".
Hero image eagerly loaded	**Fail**	Hero image has loading="lazy", which delays LCP (inferred from DOM order/size — Lighthouse LCP element unavailable). Use loading="eager" (or omit loading) and add fetchpriority="high".
Hero is a real (not a CSS background-image)	N/A	No CSS background-images detected on raster-image-eligible elements.
Responsive images (srcset /)	**Pass**	20/20 raster images use srcset or (100%).
Reasonable number of image sizes	**Pass**	48 distinct srcset widths.
JS scripts not blocking in	**Warn**	1 render-blocking script in . Move to footer or add defer/async.

Fixes

Priority 1: Critical

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

1A. Force HTTPS redirect for all HTTP traffic

- **Impact:** Security, Data Integrity
- **Problem:** http://demo.playandnope.com/ does not redirect to HTTPS, leaving users vulnerable to MITM attacks on unencrypted connections.
- **Solution:** Configure the web server (Apache/Nginx) to return a 301 redirect for all HTTP requests to the HTTPS version:

```
RewriteEngine On
RewriteCond %{HTTPS} off
RewriteRule ^(.*)$ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]
```

1B. Remove lazy loading from hero image

- **Impact:** LCP, FCP, Performance
- **Problem:** Hero image has loading="lazy", which delays rendering and contributes to LCP of 2.9s on mobile.
- **Solution:** Remove `loading="lazy"` from the largest above-the-fold image and add `fetchpriority="high"`:

```
<img src="hero.jpg" alt="..." fetchpriority="high" width="..."
height="...">
```

Priority 2: Important

Essential for compliance, user reach, and search visibility.

2A. Add HSTS and X-Content-Type-Options headers

- **Impact:** Security Headers Grade, Transport Security
- **Problem:** HSTS and X-Content-Type-Options are missing; Security Headers grade is 20/100.
- **Solution:** Add these headers to the server configuration:

```
Header always set Strict-Transport-Security "max-age=63072000;
includeSubDomains"
Header always set X-Content-Type-Options "nosniff"
```

2B. Fix W3C HTML validation errors

- **Impact:** Code Quality, Accessibility
- **Problem:** 10 errors found including invalid `aria-expanded` values, `target` on span, and script `type` / `defer` mismatches.
- **Solution:**
  - Set `aria-expanded="true"` or `"false"` (not empty string) on buttons.
  - Remove `target` attribute from `<span>` elements.
  - Change script `type="text/rocketlazyloadscript"` to `type="module"` or remove `defer` if not a valid MIME type.

Priority 3: Best Practice

Recommended for long-term maintainability.

3A. Implement Content-Security-Policy (CSP)

- **Impact:** XSS Defense-in-Depth

- **Problem:** CSP is missing. Site signals show no auth/payments/UGC, so this is lower priority than headers, but still recommended.
- **Solution:** Deploy a strict CSP with nonce/hash approach rather than a flat allowlist:

```
Header always set Content-Security-Policy "default-src 'self';
script-src 'nonce-{random}' 'strict-dynamic'; object-src 'none';
base-uri 'none';"
```