Audit Report: Paws N' Play – nõuanded ja artiklid lemmikloomaomanikele

Website: https://demo.playandnope.com/
Date: 07.10.2026
Audit Coverage: 98% — PageSpeed Insights: mobile: PSI HTTP 429; desktop: PSI HTTP 429
Confidence: low

Pages Audited (5 of 5):

- https://demo.playandnope.com/
- https://demo.playandnope.com/uudised
- https://demo.playandnope.com/koerad-maailma-parimad-aratuskellad-isegi-nadalavahetustel
- https://demo.playandnope.com/miks-mu-kass-vaatab-mind-nii-nagu-oleksin-idioot
- https://demo.playandnope.com/koerte-crosssfit

Summary of results

Overall Score: 78 / 100
Status: □ □ **Needs Improvement**

Site overall 78 is the mean of 4 pages. Scores range 72 (https://demo.playandnope.com/) → 82 (https://demo.playandnope.com/miks-mu-kass-vaatab-mind-nii-nagu-oleksin-idioot). Weakest page: Mobile PSI 87 and zero axe violations indicate strong core quality, but the Security basics verdict is FAILED due to missing HSTS, X-Content-Type-Options, and lack of HTTP-to-HTTPS redirect. Per the rubric, a FAILED security hygiene verdict caps the overall score below 90. Additionally, LCP is 3.1 s on mobile because the hero image uses loading="lazy", and W3C validation reports 10 errors. These security and performance gaps prevent an excellent rating despite the high accessibility score.

Per-page scores

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

Score	Performance	Accessibility	Best Practices	SEO	Security
72	87	100	96	100	FAILED

 Needs Improvement · https://demo.playandnope.com/uudised

Score	Performance	Accessibility	Best Practices	SEO	Security
76	85	100	96	100	FAILED

 Needs Improvement · https://demo.playandnope.com/koerad-maailma-parimad-aratuskellad-isegi-nadalavahetustel

Score	Performance	Accessibility	Best Practices	SEO	Security
82	90	100	96	100	FAILED

 Needs Improvement · https://demo.playandnope.com/miks-mu-kass-vaatab-mind-nii-nagu-oleksin-idioot

Score	Performance	Accessibility	Best Practices	SEO	Security
82	88	100	96	100	FAILED

— · https://demo.playandnope.com/koerte-crosssfit

Score	Performance	Accessibility	Best Practices	SEO	Security
—	—	—	—	—	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://demo.playandnope.com/	**87** / 99	**3.08 s** / 726 ms	0.000 / **0.002**
https://demo.playandnope.com/uudised	**85** / 99	**3.25 s** / 844 ms	0.000 / **0.004**

URL	Performance (M / D)	LCP (M / D)	CLS (M / D)
https://demo.playandnope.com/koerad-maailma-parimad-aratuskellad-isegi-nadalavahetustel	**90** / 99	**3.10 s** / 816 ms	**0.004** / 0.002
https://demo.playandnope.com/miks-mu-kass-vaatab-mind-nii-nagu-oleksin-idioot	**88** / 99	**3.20 s** / 836 ms	0.000 / **0.002**

Optimization Checklist

3 of 5 passing — 3 pass · 1 warn · 1 fail · 3 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	**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 /)	N/A	Only 2 raster images on the page — 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	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. Fix HTTP redirect and add baseline security headers `Security`

- **Impact:** Transport security, clickjacking, MIME sniffing
- **Problem:** Security basics FAILED: HTTP does not redirect to HTTPS, HSTS is missing, and X-Content-Type-Options is missing.
- **Solution:** Configure server to redirect HTTP to HTTPS and send these headers:

```
Header always set Strict-Transport-Security "max-age=63072000;
includeSubDomains"
Header always set X-Content-Type-Options "nosniff"
RewriteCond %{HTTPS} off
RewriteRule ^(.*)$ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]
```

1B. Harden WordPress installation `Security`

- **Impact:** Brute-force protection, information disclosure
- **Problem:** WordPress specific checks FAILED: readme.html is public, xmlrpc.php accepts POST, and user enumeration is possible.
- **Solution:**
  - Delete `/readme.html`.
  - Disable `xmlrpc.php` via `.htaccess` or plugin.
  - Use a plugin to block user enumeration (e.g., disable `?author=` queries).
  - Consider moving `wp-login.php` to a custom path.

1C. Enforce HTTP to HTTPS Redirect `Security`

- **Impact:** Transport security, MITM protection
- **Problem:** Security basics verdict FAILED: http://demo.playandnope.com/uudised does not redirect to HTTPS, leaving users vulnerable to interception.
- **Solution:** Configure the web server (Apache/Nginx) to return a 301 redirect for all HTTP requests to HTTPS:

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

1D. Remove lazy loading from hero image `Performance`

- **Impact:** LCP, FCP, Speed Index
- **Problem:** LCP is 3.2 s on mobile; the hero image has loading="lazy" which delays rendering of the largest contentful element.
- **Solution:** Remove `loading="lazy"` from the hero image and add `fetchpriority="high"`:

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

1E. Fix HTTP redirect and add baseline headers `Security`

- **Impact:** Transport security, trust, clickjacking
- **Problem:** Security Basics FAILED: HTTP does not redirect to HTTPS, HSTS is missing, and X-Content-Type-Options is missing.
- **Solution:** Configure server to redirect all HTTP traffic to HTTPS and add these headers:

```
Header always set Strict-Transport-Security "max-age=63072000;
includeSubDomains"
Header always set X-Content-Type-Options "nosniff"
Redirect permanent / https://demo.playandnope.com/
```

1F. Eager-load the hero image `Performance`

- **Impact:** LCP, FCP
- **Problem:** LCP is 3.1 s on mobile; Optimization Checklist identifies the hero image has loading="lazy" which delays LCP.
- **Solution:** Remove `loading="lazy"` from the hero image and add `fetchpriority="high"`:

```
<img src="/wp-content/uploads/.../dsc_0896-280x155.jpg" alt="..."
fetchpriority="high" width="280" height="155">
```

1G. Enforce HTTPS redirect and add baseline headers `Security`

- **Impact:** Transport security, trust, clickjacking
- **Problem:** Security Basics FAILED: HTTP does not redirect to HTTPS, HSTS is missing, and X-Content-Type-Options is missing.

- **Solution:** Configure the web server to redirect all HTTP traffic to HTTPS (301). Add the following headers:

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

Priority 2: Important

Essential for compliance, user reach, and search visibility.

2A. Optimize hero image for LCP `Performance`

- **Impact:** LCP, FCP, Speed Index
- **Problem:** LCP is 3.1 s on mobile; hero image has loading="lazy" which delays rendering.
- **Solution:** Remove `loading="lazy"` from the hero image and add `fetchpriority="high"`:

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

2B. Fix W3C HTML validation errors `Best Practices`

- **Impact:** Maintainability, potential accessibility edge cases
- **Problem:** W3C validator reports 10 errors including invalid aria-expanded values, script types, and attributes on wrong elements.
- **Solution:**
  - Fix `aria-expanded` values (must be "true" or "false", not empty).
  - Remove `defer` from scripts with non-JS MIME types.
  - Remove `target` from `<span>` elements.
  - Remove `area-hidden` from `<form>` elements.

2C. Add HSTS and X-Content-Type-Options headers `Security`

- **Impact:** Protocol downgrade protection, MIME sniffing
- **Problem:** Strict-Transport-Security and X-Content-Type-Options headers are missing, failing basic security hygiene checks.
- **Solution:** Add headers to server configuration:

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

2D. Harden WordPress installation `Security`

- **Impact:** Brute-force protection, information disclosure
- **Problem:** readme.html is public, xmlrpc.php accepts POST requests, and user enumeration is possible via /wp-json/users.
- **Solution:**
  1. Delete `/readme.html`.
  2. Disable `xmlrpc.php` in `.htaccess` or via plugin.
  3. Use a security plugin (e.g., Wordfence) to block user enumeration and restrict login attempts.

2E. Remove lazy-loading from the hero image `Performance`

- **Impact:** LCP, FCP, Mobile Performance
- **Problem:** LCP is 3.2s on mobile; the hero image has `loading="lazy"` which delays rendering of the largest contentful paint element.
- **Solution:** Update the hero `<img>` tag to use `loading="eager"` (or omit the attribute) and add `fetchpriority="high"`:

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

2F. Defer or async render-blocking scripts `Performance`

- **Impact:** FCP, TBT
- **Problem:** Optimization Checklist flagged 1 render-blocking script in `<head>`; Browser Runtime shows 1 render-blocking script.
- **Solution:** Move the script to the footer or add `defer` / `async` attributes. Ensure the script does not rely on synchronous execution order for critical rendering path.

Priority 3: Best Practice

Recommended for long-term maintainability.

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

- **Impact:** XSS defense-in-depth
- **Problem:** CSP is present but weak: missing `default-src` and `object-src 'none'`. Site signals show no auth/payments, so this is lower priority.
- **Solution:** Add `default-src 'self'` and `object-src 'none'` to the CSP header. Since this is a brochure site, a strict allowlist is less critical than baseline headers, but improves defense-in-depth.

3B. Fix W3C HTML validation errors `Best Practices`

- **Impact:** Code quality, potential rendering issues
- **Problem:** 6 errors found including invalid `type` attributes on scripts and `target` on span elements.
- **Solution:**
  1. Remove `type="text/javascript"` from standard script tags.
  2. Remove `target` attribute from `<span>` elements (use `<a>` for links).
  3. Remove `area-hidden` from `<form>` (use `aria-hidden`).

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

- **Impact:** XSS defense-in-depth
- **Problem:** CSP is present but weak (missing `default-src`, `object-src 'none'`); site signals show no auth/payments so this is lower priority.
- **Solution:** Add `default-src 'self'` and `object-src 'none'` to the existing CSP header. Use nonces for scripts if dynamic injection is needed.