WPScan Security Report — WordPress Instance (wp.98-89-111-197.sslip.io)

Scan Date: Nov 19, 2025
Tool: WPScan 3.8.28
Target: https://wp.98-89-111-197.sslip.io
IP: 98.89.111.197

---

1. Executive Summary

Your WordPress instance is up, working, and responding properly over HTTPS. WPScan successfully identified:

- WordPress **version 6.8.3** (up-to-date — excellent)
- Default WordPress theme **Twenty Twenty-Five**, version **1.2** (outdated — update recommended)
- Readme file exposed
- WP-Cron publicly accessible
- Robots.txt exposing WordPress structure
- At least **one plugin folder detected**, but version could not be determined
- No configuration backups found
- No direct vulnerability data provided (because we skipped the API token — normal for practice)

Overall risk: **Low to Medium**, mostly due to **hardening issues**, not direct vulnerabilities.

This is **exactly** what you want for PCI practice.

---

2. Key Findings (with Explanations)

2.1 Server Headers

- **Server: Apache**
  ✔ Normal for Lightsail Bitnami

2.2 robots.txt Exposed

```
/wp-admin/
/wp-admin/admin-ajax.php
```

What this means:
WordPress exposes admin paths. Normal, but it helps attackers map your structure.

PCI Impact:
Minor; relates to PCI DSS Requirement 6 (reduce information leakage).

Fix:
Add “security through obscurity” rules or leave as-is (WordPress needs admin-ajax).

2.3 WordPress readme.html Exposed

URL: `/readme.html`

Meaning:
This file reveals your WordPress version to attackers.

Fix:
In SSH:

```
sudo rm /opt/bitnami/wordpress/readme.html
```

2.4 WP-Cron Enabled (External Cron Trigger)

URL: `/wp-cron.php`

Meaning:
Attackers can repeatedly hit wp-cron.php → causes high CPU usage (DDoS vector).

Fix Option A — Disable WP cron:

```
sudo nano /opt/bitnami/wordpress/wp-config.php
```

Add:

```
define('DISABLE_WP_CRON', true);
```

Fix Option B — Set up a system cron job (best practice).

2.5 WordPress Core Version: 6.8.3

✔ **Up-to-date** — excellent
No vulnerabilities reported.

2.6 Theme: TwentyTwentyFive (Outdated)

Installed version: **1.2**
Latest version: **1.3**

Meaning:
Your default theme is outdated.

Fix:

In WP admin:

Appearance → Themes → Update

Or via SSH:

```
wp theme update twentytwentyfive
```

(WP-CLI included in Bitnami images)

2.7 Plugins

WPScan found plugin folders but not the plugin names or versions.

This means:

- Plugins are installed
- No version info = cannot confirm vulnerabilities

Fix:
Log in to WP Admin → Plugins → Update All.

---

3. Risk Rating Summary

Category	Risk	Reason
WordPress Core	**Low**	Up-to-date (6.8.3)
Theme	**Medium**	Outdated (1.2 → 1.3)
Exposed Files	**Low**	readme.html present
WP-Cron	**Medium**	Can be abused for DDoS
Plugins	**Potential Medium**	Not scanned (need API or manual check)
Server Hardening	**Medium**	Missing headers found in Nikto

---

4. PCI DSS Mapping

WPScan Finding	PCI Requirement	Explanation
Outdated theme	Req 6.2	Keep software up-to-date
readme.html exposed	Req 6.5	Information disclosure

WP-Cron open	Req 6.5.1	Denial-of-service risks
Plugins not analyzed	Req 6.3	Validate components
Missing hardening headers	Req 6.5.2	Secure coding practices

---

5. Recommended Fixes (Action Checklist)

Critical

- Update Twenty Twenty-Five theme

High

- Disable external WP-Cron
- Protect wp-cron.php via Cloudflare or .htaccess (if needed)

Medium

- Remove `readme.html`
- Add security headers (we fix this after ZAP)

Low

- Update all plugins
- Hide WordPress version in headers

---

6. Conclusion

Your WordPress Lightsail instance is **healthy**, up-to-date for core WordPress, and now fully ready for:

- ZAP scanning
- SSL Labs
- SecurityHeaders
- ClamAV
- Full PCI DSS mapping