Nikto Web Server Vulnerability Report — WordPress Lightsail PCI Practice

Date: November 19, 2025
Tool: Nikto v2.1.5
Target: `https://wp.98-89-111-197.sslip.io`
Server: Apache (Bitnami WordPress)
Scan Time: 587 seconds (≈ 9.8 minutes)

---

1. Overview

A Nikto vulnerability scan was performed against the HTTPS endpoint of the WordPress Lightsail server.
Nikto checks for thousands of known issues including:

- Outdated Apache modules
- Missing security headers
- Dangerous files and directories
- Misconfigurations
- CGI scripts
- Common web server vulnerabilities

This scan supports:

- **PCI DSS Requirement 2 — Secure configurations**
- **PCI DSS Requirement 6 — Vulnerability management**
- **PCI DSS Requirement 11 — Regular testing**

---

2. Summary of Findings

Nikto scanned **6,544 security checks** and found:

Issue	Severity	Status
Missing `X-Frame-Options` header	Medium	Needs fixing
No CGI directories found	Low/Informational	Good
13 errors during scanning	N/A	Network/timeout-related, not vulnerabilities
No major vulnerabilities	—	💚 Clean result

This is an **excellent** starting point for a PCI test environment.

---

3. Detailed Findings

3.1 Missing X-Frame-Options Header

Nikto output:

```
+ The anti-clickjacking X-Frame-Options header is not present.
```

✔ What this means (simple explanation)

Your site doesn't tell browsers:
"Don't let someone load my page inside an iframe."

Without this, attackers could try:

- *clickjacking*: tricking a user into clicking invisible buttons
- *framing attacks*: embedding your site inside theirs

🔥 Severity: Medium

This does **not** mean you're hacked — it's a standard hardening issue.

🎯 PCI Impact

This maps to:

- **PCI DSS Requirement 6.5.1** – Protection against common attacks
- **PCI DSS Requirement 6.2** – Keep systems securely configured

It's low-effort and highly recommended.

🛠️ How to fix

On Bitnami/Apache, add this to the Apache config:

```
<IfModule mod_headers.c>
    Header always append X-Frame-Options SAMEORIGIN
</IfModule>
```

Or use a WordPress security plugin later — easier for clients.

3.2 No CGI Directories Found

Nikto output:

```
+ No CGI Directories found
```

✔ This is **good** — CGI scripts are old technology and often full of vulnerabilities.
No legacy CGI = smaller attack surface.

Severity: None / Informational

3.3 13 Errors During Scan

Nikto output:

```
+ 6544 items checked: 13 error(s)
```

These errors are normal and mean:

- Minor timeouts
- SSL handshake delays
- Redirect loops
- Rate limits

They are NOT vulnerabilities.
Almost every modern server will show a few of these.

---

4. Risk Rating Summary

Category	Risk Level	Notes
Server Headers	Medium	Missing clickjacking header
Web Server Exposure	Low	Only Apache detected
Directory Structure	Low	No CGI exposed
Major Vulnerabilities	None	No exploitable findings
Overall Risk	**Low**	Good configuration

---

5. PCI DSS Mapping

PCI Requirement	Status	Notes
Requirement 1: Minimize services	PASS	Only Apache exposed
Requirement 2: Secure configurations	PARTIAL	Missing header
Requirement 6: Hardening	PARTIAL	Add X-Frame-Options
Requirement 11: Vulnerability Testing	PASS	Scan completed successfully

---

6. Recommendations

🔐 1. Add Security Header — X-Frame-Options

Use:

- `DENY` (strongest)
- or `SAMEORIGIN` (safer for WordPress)

🧹 2. Add Other Security Headers Later

Upcoming scans (SecurityHeaders.com) will also tell you to add:

- `X-Content-Type-Options`
- `Strict-Transport-Security`
- `Content-Security-Policy`
- `X-XSS-Protection`

You'll do all of these in the WordPress hardening phase (PCI Requirement 6).

🔄 3. Re-run Nikto After Hardening

When you add headers, the issue will disappear on the next scan.

---

7. Conclusion

The Nikto scan shows a **clean, low-risk WordPress setup** with only one standard hardening issue.
Your server is in excellent shape for moving forward with:

- **WPScan (WordPress vulnerabilities)**
- **OWASP ZAP (application vulnerabilities)**
- **Security Headers**
- **SSL Labs**
- **ClamAV (malware scan)**