**SSL/TLS Security Report

wp.98-89-111-197.sslip.io**

Assessment Date: Nov 19, 2025
Source: Qualys SSL Labs Server Test (Full Report Attached)

SSL Server Test_ wp.98-89-111-1…

---

1. Overall Rating

Your server scored an **A** — this is an excellent rating for SSL/TLS security.

This means:

- Strong certificate
- Strong key exchange
- Good cipher strength
- Modern TLS configuration
- No critical vulnerabilities detected

---

2. Certificate Summary

Type: EC 256-bit, signed with SHA384 (ECDSA)
Validity:

- **Issued:** Nov 19, 2025
- **Expires:** Feb 17, 2026
- **Issuer:** E7 (Let’s Encrypt intermediate)

- **Status: Trusted** by all major platforms
- **Chain Issues:** None

Notes:

- The certificate is short-term (90 days), normal for Let's Encrypt.
- No OCSP Must-Staple.
- Revocation check returned a CRL error, but the cert chain is still fully trusted.

---

3. Protocol Support

Enabled:

- **TLS 1.3** ✔
- **TLS 1.2** ✔

Disabled (Good):

- TLS 1.1 / TLS 1.0 ❌
- SSL 3 ❌
- SSL 2 ❌

This is the modern best practice configuration.

---

4. Cipher Suite Strength

TLS 1.3 ciphers (all strong):

- TLS_AES_256_GCM_SHA384

- TLS_AES_128_GCM_SHA256
- TLS_CHACHA20_POLY1305_SHA256

TLS 1.2 (strong preferred ciphers; some weak CBC ciphers still listed but **not preferred**):

- ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- ChaCha20-Poly1305

Recommendation:
→ Remove *weak CBC-based suites* if possible.
(Not required for PCI but improves the score further.)

---

5. Key Exchange

- Elliptic Curve: **x25519** and **secp256r1** supported
- Forward secrecy: **Yes (Robust)**
- DH parameter reuse: **No reuse detected**

This is excellent.

---

6. Vulnerability & Attack Checks

No vulnerabilities detected:

- **Heartbleed:** No
- **POODLE:** No
- **BEAST:** Mitigated

- **Zombie POODLE:** No
- **GoldenDoodle:** No
- **Ticketbleed:** No
- **OpenSSL CCS:** No
- **ROBOT attack:** No
- **Downgrade attacks:** Protected

Your HTTPS configuration is secure by industry standards.

---

7. Missing Security Headers

These do **not** affect the SSL grade, but affect **overall web security**:

- **Strict-Transport-Security (HSTS): Not enabled**
- **OCSP Stapling: Not enabled**
- **Public Key Pinning (HPKP): Disabled (normal)**
- **HSTS Preload: Not listed**

Recommendation:
Add this header to your Apache/Nginx:

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

This alone will give you a more hardened posture.

---

8. Server Details

- **Server:** Apache
- **HTTP/1.1 only** (supports ALPN)
- **Hostname:** ec2-98-89-111-197.compute-1.amazonaws.com

---

9. PCI DSS Significance

For PCI Requirement 4 (Encrypt cardholder data in transit), this SSL configuration meets expectations:

✔ Strong protocols (TLS 1.2/1.3)
✔ No deprecated SSL/TLS versions
✔ Strong ciphers
✔ No major vulnerabilities
✔ Trusted certificate authority

Only optional improvements for PCI-hardening:

1. Add HSTS
2. Enable OCSP Stapling
3. Remove weak CBC ciphers (TLS 1.2)

---

10. Summary Recommendations

Here are your prioritized action steps:

High Priority (Do This First)

1. **Enable HSTS**
2. **Enable OCSP Stapling**

Medium Priority

3. Remove weak TLS 1.2 CBC cipher suites
4. Enable HTTP/2 (not required, but modern)

Low Priority

5. Consider auto-renew monitoring for Let’s Encrypt
6. Confirm redirects so all traffic uses HTTPS