Web Security Assessment Report

openllm.netsectap-labs.com

Assessment Date: 2025-12-25 16:47:15 **Assessed By:** NetSecTap Security Assessment Framework **Report Version:** 1.0

Executive Summary

This security assessment evaluates the web application security posture of **openllm.netsectap-labs.com**. The assessment covers critical security controls including HTTP security headers, SSL/TLS configuration, DNS security, and technology stack analysis.

Security Findings Overview

Severity	Count
ðŸ”´ Critical	0
ðŸŸ High	1
ðŸŸ¡ Medium	1
ðŸ”µ Low	0
â„¹ï¸ Info	1

Overall Risk Rating: ðŸŸ MEDIUM RISK

Detailed Findings

Security Headers Analysis

[HIGH] Missing HTTP Strict Transport Security (HSTS) header **[MEDIUM]** Missing Content Security Policy (CSP) header **[INFO]** Server version disclosure detected

---

Technical Assessment Details

Assessment Data for openllm.netsectap-labs.com

Assessment Date: 2025-12-25

DNS Information

172.67.173.252 104.21.96.66

Security Headers

HTTP/2 403 date: Thu, 25 Dec 2025 16:47:10 GMT content-type: text/html; charset=UTF-8 accept-ch: Sec-CH-UA-Bitness, Sec-CH-UA-Arch, Sec-CH-UA-Full-Version, Sec-CH-UA-Mobile, Sec-CH-UA-Model, Sec-CH-UA-Platform-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Platform, Sec-CH-UA, UA-Bitness, UA-Arch, UA-Full-Version, UA-Mobile, UA-Model, UA-Platform-Version, UA-Platform, UA cf-mitigated: challenge critical-ch: Sec-CH-UA-Bitness, Sec-CH-UA-Arch, Sec-CH-UA-Full-Version, Sec-CH-UA-Mobile, Sec-CH-UA-Model, Sec-CH-UA-Platform-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Platform, Sec-CH-UA, UA-Bitness, UA-Arch, UA-Full-Version, UA-Mobile, UA-Model, UA-Platform-Version, UA-Platform, UA cross-origin-embedder-policy: require-corp cross-origin-opener-policy: same-origin cross-origin-resource-policy: same-origin origin-agent-cluster: ?1 permissions-policy: accelerometer=(),browsing-topics=(),camera=(),clipboard-read=(),clipboard-write=(),geolocation=(),gyroscope=(),hid=(),interest-cohort=(),magnetometer=(),microphone=(),payment=(),publickey-credentials-get=(),screen-wake-lock=(),serial=(),sync-xhr=(),usb=() referrer-policy: same-origin server-timing: chlray;desc=â€œ9b39d19d594476b0â€ x-content-type-options: nosniff x-frame-options: SAMEORIGIN cache-control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0 expires: Thu, 01 Jan 1970 00:00:01 GMT report-to: {â€œendpointsâ€: [{â€œurlâ€:â€œhttps://a.nel.cloudflare.com/report/v4?s=6b8tham2eVpxCHSrNDd9hE9Qfkc7m4y%2BW497MQ7FVqYGdkXlVnhJJVL17goqiKj9QGx0k%2F9WOZRQz5YHAS6OkyL4cVCJfKxBFZ4DYiQMrYBwBMIsOJb%2B%2BpLzhe%2BcMecpZEhtWKynelâ€,â€œmax_ageâ€:604800} nel: {â€œsuccess_fractionâ€:0,â€œreport_toâ€:â€œcf-nelâ€,â€œmax_ageâ€:604800} server: cloudflare cf-ray: 9b39d19d594476b0-SEA alt-svc: h3=â€œ:443â€; ma=86400 server-timing: cfL4;desc=â€œ?proto=TCP&rtt=2964&min_rtt=1708&rtt_var=1223&sent=7&recv=10&lost=0&retrans=0&sent_bytes=3431&recv_bytes=788&delivery_rate=2218321&cwnd=253&unsent_bytes=0&cid=c42e

Technology Stack

https://openllm.netsectap-labs.com/ [403 Forbidden] Country[RESERVED][ZZ], HTML5, HTTPServer[cloudflare], IP[172.67.173.252], Script, Title[Just a momentâ€¦], UncommonHeaders[accept-ch,cf-mitigated,critical-ch,cross-origin-embedder-policy,cross-origin-opener-policy,cross-origin-resource-policy,origin-agent-cluster,permissions-policy,referrer-policy,server-timing,x-content-type-options,report-to,nel,cf-ray,alt-svc], X-Frame-Options[SAMEORIGIN], X-UA-Compatible[IE=Edge]

SSL Certificate

notBefore=Dec 19 09:45:37 2025 GMT notAfter=Mar 19 07:54:44 2026 GMT issuer=C = US, O = Google Trust Services, CN = WE1 subject=CN = netsectap-labs.com

---

Recommendations

Priority 1: Critical & High Severity

1. **Enable HSTS (HTTP Strict Transport Security)**
   - Add header: `Strict-Transport-Security: max-age=31536000; includeSubDomains; preload`
   - Prevents protocol downgrade attacks and cookie hijacking
   - Implementation: Configure web server to send HSTS header on all HTTPS responses
2. **Implement Content Security Policy**
   - Add restrictive CSP header to prevent XSS attacks
   - Start with: `Content-Security-Policy: default-src 'self'; script-src 'self'`
   - Gradually refine policy based on application requirements

Priority 2: Medium Severity

3. **Add Clickjacking Protection**
   - Implement: `X-Frame-Options: DENY` or `X-Frame-Options: SAMEORIGIN`
   - Prevents UI redress attacks
4. **Enable MIME-Type Sniffing Protection**
   - Add: `X-Content-Type-Options: nosniff`
   - Prevents browsers from MIME-sniffing responses

Priority 3: Informational

5. **Remove Server Version Headers**
   - Disable server version disclosure in HTTP headers
   - Reduces information leakage for potential attackers

Next Steps

1. Review and prioritize findings based on business risk
2. Implement Priority 1 recommendations immediately
3. Plan implementation timeline for medium severity items
4. Re-test after implementing fixes
5. Consider implementing automated security header monitoring

---

Assessment Methodology

This assessment was performed using automated tools and manual verification: - DNS reconnaissance - HTTP security header analysis - SSL/TLS configuration review - Technology stack fingerprinting - OWASP Top 10 security control validation

Note: This is an automated assessment. For comprehensive security testing, consider a full penetration test.

Report generated by NetSecTap Security Assessment Framework For questions or clarifications, please contact your security team