

API



PENTESTING

External Pentest

Penetration Test on <https://system.visionxlab.com/api/>, consumer landing pages

Completed 10/23/2026

Third-Party Independence Attestation

To Whom It May Concern:

This letter confirms that MSP Pentesting LLC (also operating as Affordable Pentesting) is an independent, US-based third-party penetration testing firm engaged by M4 Labs LLC to perform security testing of its VisionXLab lead-generation platform.

Test type:

External, authenticated (grey-box) web application and API penetration test, including vulnerability scanning of internet-facing systems.

Dates:

Testing was conducted from October 19 to October 23, 2026.

Scope:

- Application: consumer landing pages and lead forms, and the admin application
- APIs: API gateway (system.visionxlab.com/api) and backend edge functions
- Access controls: authentication, two-factor authentication, authorization, and database row-level security
- Integrations and data flows: lead delivery to client CRMs and the no-data-retention lead path
- Environment configuration: TLS, security headers and secrets management

Methodology:

Testing followed the OWASP Testing Guide, NIST SP 800-115 and PTES-aligned manual testing, supplemented by automated tooling.

Results:

No Critical, High or Medium severity findings were identified. One Low severity finding and one Informational finding were reported to M4 Labs LLC in the Penetration Test Report v1.1, dated October 23, 2026.

Critical	High	Medium	Low	Informational
0	0	0	1	1

Verified controls:

No personal data was retrievable on the no-data-retention lead path.
Database access is deny-by-default and no row-level security bypass was found.
Lead routing could not be altered after intake. Update tokens were enforced.

Remediation status:

One Low severity finding was identified and reported to M4 Labs LLC with a remediation recommendation.

Tester:

The assessment was performed by Zachary ElMetennani, CySA+, Security Lead at MSP Pentesting LLC.

MSP Pentesting LLC operates fully independently of M4 Labs LLC. All testing, findings and reporting were conducted solely by MSP Pentesting LLC personnel. This separation ensures the penetration test was conducted with full independence and objectivity, consistent with industry best practices for third-party security assessments.

Zachary ElMetennani - October 23, 2026

Security Lead, CySA+

MSP Pentesting LLC

zack@affordablepentesting.com

www.affordablepentesting.com, www.msppentesting.com



Appendix

The MSP Pentesting team used the following standards to rate the findings in the report. MSP Pentesting LLC derived these risk ratings from the industry and organizations such as OWASP & the Common Weakness Enumeration (CWE) ratings.

Severity Descriptions

The severity of each finding in this report is independent. Finding severity ratings combines direct technical and business impact with the worst-case scenario in an attack chain. The more significant the impact, and the fewer vulnerabilities that must be exploited to achieve that impact, the higher the severity.

Critical

Vulnerability is an otherwise high-severity issue with additional security implications that could lead to exceptional business impact. Examples: trivial exploit difficulty, business-critical data compromised, bypass of security controls, direct violation of communicated security objectives, and large- scale vulnerability exposure.

High

Vulnerability may result in direct exposure including, but not limited to: the loss of application control, execution of malicious code, or compromise of underlying host systems. The issue may also create a breach in the confidentiality or integrity of sensitive business data, customer information, and administrative and user accounts. In some instances, this exposure may extend farther in the infrastructure beyond the data and systems associated with the application.

Medium

Vulnerability does not lead directly to the exposure of critical application functionality, sensitive business and customer data, or application credentials. However, it can be executed multiple times or leveraged in conjunction with another issue to cause direct exposure. Examples include brute-forcing and client-side input validation.

Low

Vulnerability may result in limited exposure of application control, sensitive business and customer data, or system information. This type of issue provides value only when combined with one or more issues of a higher risk classification. Examples include overly detailed error messages, the disclosure of system versioning information, and minor reliability issues.

Informational

A security-relevant observation that does not present a direct, exploitable risk on its own but is worth noting for defense-in-depth or hardening purposes.