aikido

09 October 2026

Penetration Test Report

SpeakAI Web Application Whitebox Security Assessment

For speakai

Table of Contents

Report Overview 3

Remaining Risk 4

Risk Posture 5

About This Pentest

Report Overview

Date

09 October 2026

Test Type

white box

Client

speakai

Engagement Summary

On 09 October 2026, Aikido conducted a white box web application penetration test for speakai focused on the application(s) within the defined scope and their exposure to targeted attacks. The primary goal of this engagement was to proactively discover vulnerabilities within those scoped applications that could lead to compromise or exposure of sensitive information.

The penetration test simulated real-world attack techniques across applicable attack surfaces, including authentication, authorization, input handling, business logic, and where relevant, agentic and API-specific behaviors, to identify risks within the scoped application(s). The configured scope was limited to the following domains and associated endpoints:

Scope

- **https://app.speakai.co**
- **https://api.speakai.co**
- **https://storage.speakai.co**

Security Posture

Remaining Risk

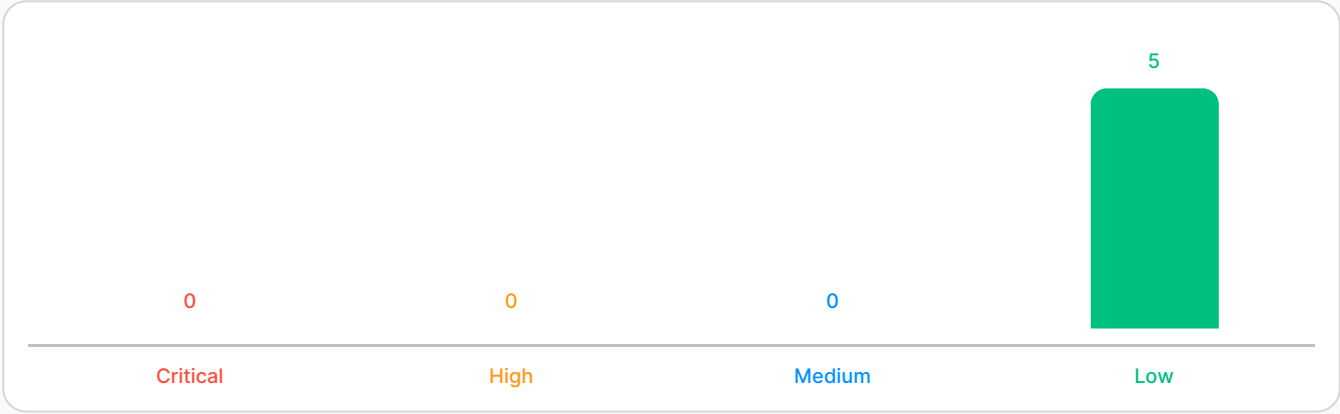
Following remediation, **5 findings** remain open across the tested scope. Continued improvements are recommended to reduce residual exposure.

Detailed findings and remediation evidence are documented in the full penetration test report.

Current Status

Avg. Resolution Time	Highest Severity	Unresolved Issues
38 days	Low	5
		5 Low

Open Issues by Severity



Conclusion

Risk Posture

Rating Scale

A	Excellent	Exceeding best practices
B	Good	Meeting industry standards
C	Fair	Moderate improvements needed
D	Poor	Significant attack surface
F	Critical	Immediate remediation required

After Remediation



Excellent

Security posture for this scope aligns with strong baseline expectations.