

Waversoft: security audit report

Created on 19 October 2026 @ 08:19

Waversoft wants to build trust by giving you insight in how it builds software in a secure manner. The report details how software development at Waversoft is being monitored and safeguarded from the developer's computer all the way to the infrastructure used for delivery.

This security report has been generated by Aikido Security based on real-time monitoring of Waversoft code and infrastructure.



OWASP Top 10

This section details the OWASP risks for which the organization currently has active measures against.

Code	Title	Taken measures
A01:2025	Broken access control	✓ Principle of least privilege applied for cloud users ✓ Application is properly configured ✓ Prevents unauthorized access to resources ✓ App protected against SSRF attack opportunities
A02:2025	Security misconfiguration	✓ Application is properly configured
A03:2025	Software Supply Chain Failures	✓ Code repositories use lockfiles to pin dependencies ✓ Not affected by malware issues
A04:2025	Cryptographic failures	✓ Enforces encryption of data at rest ✓ Enforces the use of secure connections ✓ Prevents the exposure of secret keys
A05:2025	Injection	✓ App scanned for SQL injection attack ✓ Prevents remote code execution ✓ Prevents CSRF attacks ✓ Prevents Cross Site Scripting (XSS) ✓ Prevents command injection
A06:2025	Insecure design	✓ Configured monitoring for code repositories
A07:2025	Authentication Failures	✓ Prevents bypassing authorization controls ✓ Prevents improper certificate validation
A08:2025	Software or Data Integrity Failures	✓ Code repositories use lockfiles to pin dependencies ✓ Takes measures to ensure proper deserialization
A09:2025	Security Logging and Alerting Failures	✓ Has enabled notification integration
A10:2025	Mishandling of Exceptional Conditions	✓ Properly handle exceptional conditions



SLA compliance report

The table below shows the configured SLAs and pinpoints instances shows the amount of issues that do currently do not meet these standards.

Issue priority level	SLA	# Issues too late
Critical	5 days	0
High	20 days	0
Medium	60 days	0
Low	100 days	0

HIPAA compliance

A brief overview of the HIPAA Compliance Checklist and any measures taken for these.

Title	Taken measures
1.3.1 Security Standards: General Requirements	✔ Encrypts data at rest ✔ Enforces safe SSL protocol usage ✔ Enforces latest TLS version ✔ Prevents abuse of cookies ✔ Uses up to date cryptography libraries
1.4.1 Administrative Safeguards: Security management process	✔ Enabled security logging for cloud instances ✔ Configured SLAs to resolve issues
1.4.4 Administrative Safeguards: Information access management	✔ Applies the least privilege principle for cloud users ✔ Applies the least privilege principle for cloud resource
1.4.5 Administrative Safeguards: Security awareness and training	✔ Enabled security logging for cloud instances
1.4.7 Administrative Safeguards: Contingency plan	✔ Has backups for stateful cloud resources
1.6.1 Technical Safeguards: Access control	✔ Applies the least privilege principle for cloud users ✔ Applies the least privilege principle for cloud resource
1.6.2 Technical Safeguards: Audit controls	✔ Enabled security logging for cloud instances
1.6.3 Technical Safeguards: Integrity	✔ Encrypts data at rest ✔ Uses up to date cryptography libraries
1.6.4 Technical Safeguards: Person or entity authentication	✔ Applies the least privilege principle for cloud resource ✔ Applies the least privilege principle for cloud users



1.6.5 Technical Safeguards:
Transmission Security

- ✓ Encrypts data at rest
- ✓ Uses up to date cryptography libraries
- ✓ Enforces safe SSL protocol usage
- ✓ Enforces latest TLS version
- ✓ Prevents abuse of cookies



Scan history report

This section details all company assets that are being monitored and how often scans are performed.

Kind	Frequency	Last occurrence
Open-source dependencies: 902 JavaScript packages monitored 7 swift packages monitored	Daily	2026-10-19
OSS licenses: 909 monitored for compliance	Weekly	2026-10-19
Static app security testing: 1 repository monitored	Daily	2026-10-19
Infrastructure as code: monitored for misconfigurations	Daily	2026-10-19
Exposed secrets: history of 1 repository scanned	Daily	2026-10-19
Cloud misconfiguration checks: 1 cloud scanned	Daily	2026-10-19
Domains: 1 monitored for known vulnerabilities	Daily	1970-01-01



Issue insights over the past 3 months

The table below gives an overview of new findings in a 3 month rolling window. A triaged finding is one that has been either been solved, ignored after analysis or planned in a task management system for resolution.

Issue kind	New	False positives	Handled
Open-source Dependencies	1	1	0
Container Images	0	0	0
Cloud Configurations	11	0	0
Virtual Machines	0	0	0
Secrets in source code history	2	0	0
DAST/Surface Monitoring	0	0	0
SAST/Static App Security Testing	83	0	0
Infrastructure As Code	0	0	0
Mobile	0	0	0
End-of-life Runtimes	0	0	0
Access Controls	0	0	0
Licenses	0	0	0
Malware Issues	0	0	0
AI Pentest Issues	75	0	7



Cloud compliance report

This report shows an overview of all the cloud posture rules the company complies with.

Provider	Rule	Status
 Supabase	Supabase refresh token rotation is enabled	Compliant
 Supabase	Supabase functions do not rely on legacy JWT verification	Compliant