V703-Art: security audit report

Created on 25 November 2025 @ 03:51

V703-Art wants to build trust by giving you insight in how it builds software in a secure manner. The report details how software development at V703-Art 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 V703-Art 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
A01:2021	Broken access control	✓ Application is properly configured ✓ Prevents unauthorized access to resources
A02:2021	Cryptographic failures	✓ Enforces encryption of data at rest ✓ Enforces the use of secure connections ✓ Prevents the exposure of secret keys
A03:2021	Injection	✓ App scanned for SQL injection attack ✓ Prevents remote code execution ✓ Prevents CSRF attacks ✓ Prevents Cross Site Scripting (XSS) ✓ Prevents command injection
A04:2021	Insecure design	✓ Configured monitoring for code repositories
A05:2021	Security misconfiguration	✓ Application is properly configured
A06:2021	Vulnerable and Outdated Components	Monitoring, not fully compliant
A07:2021	Identification and Authentication Failures	✓ Prevents bypassing authorization controls ✓ Prevents improper certificate validation
A08:2021	Software and Data Integrity Failures	✓ Code repositories use lockfiles to pin dependencies ✓ Takes measures to ensure proper deserialization
A09:2021	Security Logging and Monitoring Failures	Monitoring, not fully compliant
A10:2021	Server-Side Request Forgery	✓ App scanned for SSRF attack opportunities

Scan history report

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

Kind	Frequency	Last occurence
Open-source dependencies:	Daily	No scan occured yet
OSS licenses: 0 monitored for compliance	Weekly	No scan occured yet
Static app security testing: 0 repositories monitored	Daily	No scan occured yet
Infrastructure as code: monitored for misconfigurations	Daily	No scan occured yet
Exposed secrets: history of 0 repositories scanned	Daily	No scan occured yet

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	0	0	0
Container Images	0	0	0
Cloud Configurations	0	0	0
Virtual Machines	0	0	0
Secrets in source code history	0	0	0
DAST/Surface Monitoring	0	0	0
SAST/Static App Security Testing	0	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	0	0	0