R5-App: security audit report

Created on 04 February 2026 @ 19:08

R5-App wants to build trust by giving you insight in how it builds software in a secure manner. The report details how software development at R5-App 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 R5-App code and infrastructure.

Aikido benchmark

This percentage gives an indication of your security posture as a company, compared to all other Aikido customers.

Top
5%
of accounts

Section	Score
Score for code repositories	Top 5%
Score for cloud environment	N/A

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A06:2021	Vulnerable and Outdated Components	Monitoring, not fully compliant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	✓ Has email notifications set up
A10:2021	Server-Side Request Forgery	✓ App scanned for SSRF attack opportunities

ISO 27001:2022 compliance

A brief overview of the ISO 27001 requirements and any measures taken for these.

Title	Taken measures
A.8.2 - Privileged access rights	Monitoring, not fully compliant
A.8.3 - Information access restriction	Monitoring, not fully compliant
A.8.5 - Secure authentication	Monitoring, not fully compliant
A.8.6 - Capacity management	Monitoring, not fully compliant
A.8.7 - Protection against malware	✓ Prevents unwanted write operations to filesystems ✓ Uses Lockfiles to pin code dependencies
A.8.8 - Management of technical vulnerabilities	Monitoring, not fully compliant
A.8.12 - Data leakage prevention	✓ Prevents remote code execution ✓ Has measures against SQL injection attacks ✓ Prevents XSS attacks
A.8.13 - Backups	Monitoring, not fully compliant
A.8.15 - Logging	Monitoring, not fully compliant
A.8.18 - Use of privileged utility programs	✓ Prevents the exposure of sensitive data
A.8.20 - Network security	Monitoring, not fully compliant
A.8.31 - Separation of development, test and production environments	Monitoring, not fully compliant
A.8.24 - Use of cryptography	✓ Uses secure cookies ✓ Uses up-to-date cryptographic libraries

A.8.9 - Configuration management	✓ Uses Lockfiles to pin code dependencies
A.8.16 - Monitoring activities	✓ Receives security alerts in real time
A.8.25 - Secure development lifecycle	✓ Has connected a code repository
A.8.28 - Secure coding	Monitoring, not fully compliant
A.8.32 - Change management	Monitoring, not fully compliant
A.5.15 - Access control	✓ Prevents the exposure of sensitive data
A.5.16 - Identity management	Monitoring, not fully compliant
A.5.28 - Collection of evidence	Monitoring, not fully compliant
A.5.33 - Protection of records	Monitoring, not fully compliant

GDPR compliance

A brief overview of GDPR rules and any measures taken for these.

Title	Taken measures
2.1 Principles Relating to Processing of Personal Data	✓ Use of Cryptography: Enforces SSL ✓ Use of Cryptography: Secure Cookies ✓ Use of Cryptography Libraries
4.2 Data Protection by Design	Monitoring, not fully compliant
4.5 Processor	✓ Use of Cryptography: Enforces SSL ✓ Use of Cryptography: Secure Cookies ✓ Use of Cryptography Libraries
4.7 Records of Processing Activities	Monitoring, not fully compliant
4.9 Security of Processing	✓ Use of Cryptography: Enforces SSL ✓ Use of Cryptography: Secure Cookies ✓ Use of Cryptography Libraries

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: • 969 JavaScript packages monitored	Daily	2026-02-04
OSS licenses: 969 monitored for compliance	Weekly	2026-02-04
Static app security testing: 2 repositories monitored	Daily	2026-02-04
Infrastructure as code: monitored for misconfigurations	Daily	2026-02-04
Exposed secrets: history of 2 repositories scanned	Daily	2026-02-04
Domains: 1 monitored for known vulnerabilities	Daily	2026-02-04

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	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	4	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