Sparrow **SAST** / **SAQT**

A Smart & Secure DevSecOps

Sparrow SAST/SAQT efficiently detects and resolves security vulnerabilities and quality issues within source code. By automating semantic-based testing, it frees up developers' time for critical tasks, ensuring that code is thoroughly reviewed and fixed before release.

Comprehensive Language Coverage

Practical Management Options

On-Premises and Cloud

Auto–Tracking

Features over 2,300 security and quality checkers for 26 languages, including C, C++, Java, TypeScript, Go, Rust, Dart, Kotlin, Lua, C# and Python. Sparrow SAST/SAQT ensures compliances with global security and quality standards.

Sparrow SAST/SAQT delivers in-depth analysis and remediation recommendations for identified security and quality issues.
It offers comprehensive management features, including checkers management, issues tracking, and user role or permission control.
All these features are accessible through a convenient web interface.

Sparrow SAST/SAQT is available as an on-premises solution, a cloud-based SaaS offering, or an API. Customers can select the deployment option that best suits their application development environment.

Sparrow SAST/SAQT automatically scans application for security vulnerabilities and quality issues, and tracks changes in their status, and helps users to efficiently manage similar issues.

SPARROW

Sparrow SAST

▶ Features

- Supports 20+ languages: C/C++, Java, JSP, C#, Rust, Go, PHP, Python, Swift, Visualforce, Android Java, Objective-C, HTML, SQL, ABAP, ASP.NET, VB.NET, JavaScript, Lua, VBScript, TypeScript, Kotlin, Dart, Pro-C, XML

- Plugins for Eclipse, IntelliJ, Visual Studio, Android Studio, Eclipse Based Tool (IBM RAD), Proframe Studio, Visual Studio Code

- Checks major security and quality references.

- Tracks and manages vulnerabilities with Issue Navigator.

- Provides automated correction guides with Active Suggestion.

- Supports customized reports (PDF, Word, Excel, CSV).

About Us

Since 2007, Sparrow Co. Ltd., has been developing comprehensive software security solutions based on its exclusive technical knowledge. Our products consist of complete packages about application security testing solutions to implement a smart and secure DevSecOps. Our group of experts provides fully managed both on-premises and cloud-based tools to carry out a perfect SDLC.

SPARROW

▶ Supported Environments

Operating System

- Server : Windows 10 or later
  Ubuntu 12.04 or later
  Fedora 24 or later
  CentOS 6.8 or later
  Rocky 8.9 or later
  RHEL 5 or later
  MacOS 10~14
  Oracle 8.9
  Debian 11
  HPUX 11.31

- Client : Windows 10 or later
  Ubuntu 12.04 or later
  CentOS 6.8 or later
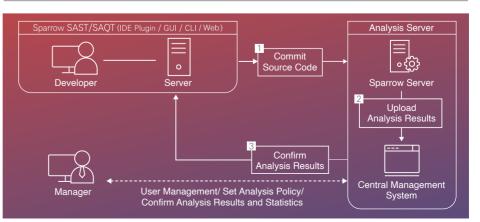 Rocky 8.9 or later
  MacOS 10~14

Framework

- iBatis 3.0, MiPlatform 3.3, MyBatis 3.3, Nexacro 14, Node.js 14.0, Proframe, React, Spring Framework 3, Struts Framework 4.0, Vue.js 2, 3, XPlatform 3, 9.2

Plugin

- Android Studio 2020.3.1.25, 4.0, 4.11
  Proframe Studio 4.0, 5.0
  Visual Studio 2013, 2015, 2017, 2019, 2022
  Visual Studio Code 1.62.2, 1.83.1
  InteliJ 20.1, 20.2, 21.2, 21.3, 22.1, 22.3, 23.1, 23.2
  Eclipse Luna, Kepler, 2020-06, 2021-09, 2022-06, 2023-09, 2023-12

System Requirements

	Server	Client
CPU	Quad Core 2.5GHz	Dual Core 2GHz
RAM	16GB	2GB
HDD	300GB	3 GB + (2x amount of testing codes)

Supported Reference

.NET Framework Design Guideline	HIC++ 2.2
BSSC C/C++ 2000	HIS 1.0.3
CERT-C/C++	IEC 61508-Exida C/C++
CERT-JAVA	ISO 26262
CWE	JPL
CWE 658 List	MISRA-C++:2008
CWE 659 List	MISRA-C:1998
CWE 660 List	MISRA-C:2004
MISRA-C:2012 (Amend. 2, 3)	Code Conventions for the Java Programming Language (Oracle)
MSDN C#:2015	PCI DSS
OWASP 2017, 2021	Visual Studio 2015 Code Warnings
CERT-C/C++ 2016 Edition	Rust ANSSI guide v1.0

	On-Premises	Cloud
Static Application Security Testing	O	O
Static Application Quality Testing	O	O
Dashboard	O	O
Correction Guide (Active Suggestion)	O	O
C/C++ Analysis	O	O (Only with default compiler)
Customizable Report (PDF, Excel, CSV, Word)	O	Not customizable
International Compliance Reference	O	O
Non-Compiled Language Analysis	O	O
Incremental Analysis	O	X
User Role & Permission	O	X
IDE Integration	O	X
CLI / Batch Analysis	O	X
Customizable Checker Group	O	X
Compatible with LDAP / Redmine / Jira	O	X