

# Sparrow SAST

## A Smart & Secure DevSecOps

Sparrow SAST (Static Application Security Testing) identifies and eliminates security vulnerabilities or quality issues (i.e. buffer overflow) of source code. As application developers run out of time to review the source code in between product releases and updates, this semantic based testing tool will help them swiftly find and fix the code.



### Comprehensive Language Coverage

More than 2,300 security vulnerability checkers across 24 languages, including C, C++, Java, and JSP. Sparrow SAST supplies checkers satisfying global security compliance guides and standards.



### Practical Management Options

Sparrow SAST gives specific suggestions for detected security vulnerabilities. It allows you to manage checkers, security vulnerability issues, and roles or permissions of users for each project. These management options are controlled on a web browser.



### On-Premise and Cloud

Sparrow SAST is available both on-premise and cloud. Customers can choose between them based on their application development environments.



### Auto-Tracking

Sparrow SAST automatically checks application security vulnerabilities, tracks changed states of issues, and applies them to comparable subsequent issues.

# Sparrow SAST

## ► Features

- Supports 24 languages: C/C++, Java, JSP, C#, XML, PHP, Python, Swift, Apex, Visualforce, Android Java, Objective-C, HTML, SQL, ABAP, ASP.NET, VB.NET, JavaScript, VBScript, XSL, TypeScript, Go, Kotlin
- Plugins for Eclipse, IntelliJ, Visual Studio, Android Studio, Eclipse Based Tool (IBM RAD), Proframe Studio.
- Checks major security and quality references.
- Tracks and manages vulnerabilities with Issue Navigator.
- Provides automated correction on Active Suggestion.
- Supports customized reports (PDF, Word, Excel, CSV).

## ► Supported Environments

### Operating System

- Server : Windows Server 2000 or above, Ubuntu 8.04 or above, RedHat Linux 5 or above, Fedora 8 or above, CentOS 5 or above
- Client : Windows XP or above, Ubuntu 8.04 or above, RedHat Linux 5 or above, Fedora 8 or above, CentOS 5 or above, AIX 6.1 or above, HP\_UX 11.23 or above, SUN\_OS 5.10 or above, Mac\_OS 10.6 or above

### Language

- C, C++, Java, JSP, C#, XML, PHP, ASP.NET, VB.NET, JavaScript, VBScript, Android Java, Objective-C, HTML, SQL, ABAP, Python, Swift, Apex, Visualforce, XSL, TypeScript, Go, Kotlin

### Framework

- Spring Framework, iBATIS, MyBatis, Struts2, ASP.NET MVC, Tmax Proframe

### System Requirements

	Server	Client
CPU	Quad Core 2.5GHz	Dual Core 2GHz
RAM	16GB	2GB
HDD	300GB	500 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	Oracle
MSDN C#:2015 Coding Rules	PCI DSS
OWASP	Visual Studio 2015 Code Warnings

## 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-premise and cloud-based tools to carry out a perfect SDLC.

	On-Premise	Cloud
Static Application Security Testing	O	O
Static Application Quality Testing	O	O
Dashboard	O	O
Correction Guide (Active Suggestion)	O	O
Customizable Report (PDF, Excel, CSV, Word)	O	O
International Compliance Reference	O	O
Non-Complied Language Analysis	O	O
Incremental Analysis	O	O
User Role & Permission	O	X
IDE Integration	O	X
C/C++ Analysis	O	X
CLI / Batch Analysis	O	X
Customizable Checker Group	O	X
Compatible with LDAP / Redmine / Jira	O	X