



Companies rely on web applications to stock a portion of business information or to run the entire business. If web security threats are raised, these will bring increasingly large damage. Although securing online services and linked data is indispensable for the companies, a recent statistics shows that they are unprepared, and keep losing capacities to respond to unstoppable challenges.

A Smart & Secure DevSecOps

For companies who try to conduct a secure web application, Sparrow offers a series of tools to manage security vulnerabilities throughout SDLC (Software Development Lifecycle).

Comprehensive Coverage

Provides software packages to cover application security through development, testing and operation process. Compatible with various systems.

Manageability

Helps control users' roles and permissions for projects on a web browser. Equipped with useful plugins and options.

Flexibility

Support both on-premises and cloud. Customers can choose between them based on their application development environments.

Automation

Automatically checks application security vulnerabilities and suggests alternatives.

90%

Sites vulnerable to application attacks

*Source: RSA Conference 2016

53%

IT organizations believe they're short of existing skills about cybersecurity

*Source: Oracle and KPMG Cloud Threat Report 2019

\$10

Cybercrime tools and kits you can buy on the Dark Web and online marketplace

*Source: ZDNet articles

200

Average days to detect security breach

*Source: Microsoft Official Blog

Sparrow SAST

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.

Highlights

- More than 2,300 security vulnerability checkers across 21 languages.
- Whole management options are controlled on a web browser.
- Available as on-premise and cloud.
- Checks application security vulnerabilities, tracks changed states of issues, and applies them to comparable subsequent issues.

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

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

Framework

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

IDE Integration

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

Sparrow DAST

Sparrow DAST (Dynamic Application Security Testing) detects security vulnerabilities with more than 1,400 web application checkers. It also delivers IAST (Interactive Application Security Testing) by scanning web applications with Truescan agent (an RASP module). Moreover, Sparrow DAST enables you to schedule a testing plan for a project to save your time.

Highlights

- Calculates possible threat routes with more than 1,400 web application checkers.
- Performs an integrity test with ReCheck option to save testing time.
- Provides Event Clipboard to record and replay analysis information for detecting and sharing the exact events.
- Available as on-premise and cloud.

	On-Premise	Cloud
Vulnerability Check with HTML5 / Ajax	O	O
Dashboard	O	O
Event Clipboard	O	O
IAST Module Testing (Truescan)	O	O
Customizable Report (Word, Excel, PDF, HTML, CSV)	O	O
International Compliance Reference	O	O
ReCheck	O	X
User Role & Permission	O	X
Customizable Checker Group	O	X
Compatible with LDAP	O	X

► Supported Environments

Operating System

- Windows 7 or above, Windows Server 2000 or above, RedHat Linux 7 or above, CentOS 7 or above, Ubuntu 14.04 or above, Debian 8 or above, OpenSUSE 13.3 or above, Fedora 24 or above

Sparrow RASP

Unlike a WAF (Web Application Firewall), Sparrow RASP (Runtime Application Self-Protection) uses an application runtime environment itself to monitor real-time external requests and internal responses, and then implement self-protection. It identifies more accurate security threats, makes alarms, blocks them against cyber-attacks, and even more, it patches the application to prevent damage.

Highlights

- Supports a Java-based application in various WAS (Web Application Servers).
- Provides an activate or deactivate option on a web browser.
- Causes minimum impact on the application performance.
- Automatically monitors attacks or exploits on unexpected vulnerabilities of the application.

Supported Environments

Operating System

- Windows Server 2000 or above, Ubuntu 8.04 or above, RedHat Linux5 or above, Fedora8 or above, CentOS 5 or above

WAS

- Tomcat, Jetty, JBoss AS, Wildfly, WebLogic, WebSphere Liberty, Profile, JEUS, etc.

Framework

- Spring Framework, iBATIS, MyBatis, Hibernate

JDBC Driver

- Oracle, SQL Server, MySQL, PostgreSQL, MariaDB, HyperSQL, etc.

Sparrow InteractiveHUB

Sparrow InteractiveHUB is an integrated solution that improves performance and remediation process with related information about vulnerabilities detected in Sparrow SAST, Sparrow DAST and Sparrow RASP. It is the perfect solution to check your application security at various angles throughout the entire SDLC (Software Development Lifecycle).

Highlights

- Manages security vulnerabilities detected during web application development, testing, and operation.
- Provides APIs to work with other tools and supports statistics, indicator, and trending graphs.

Supported Environments

Operating System

- Windows Server 2000 or above, Ubuntu 8.04 or above, Redhat Linux5 or above, Fedora8 or above, CentOS 5 or above

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.