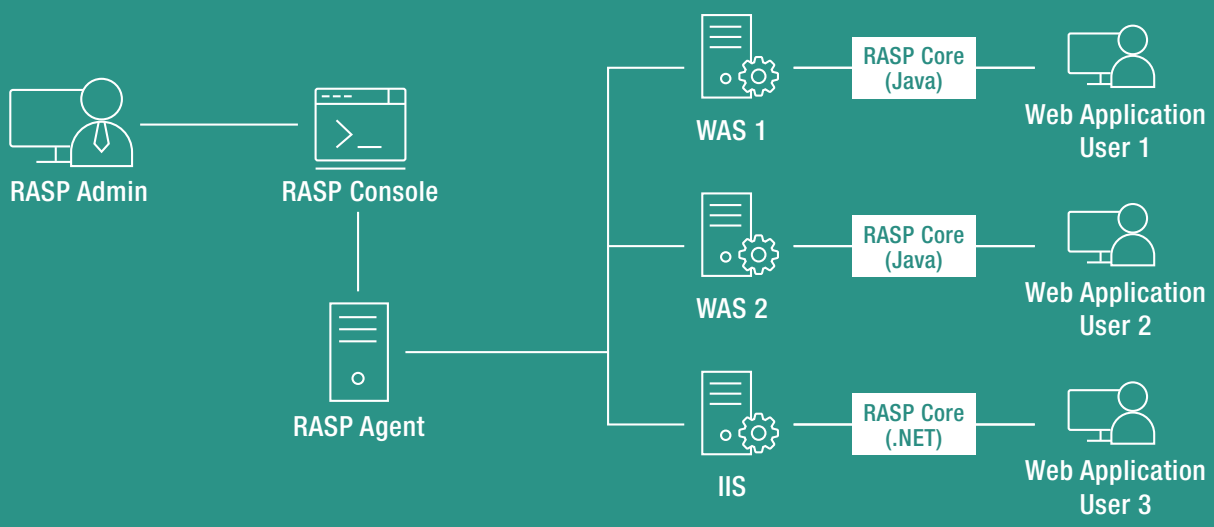
RASP Sparrow

Detect & block attacks against applications in a runtime environment



Web Management

- Track all external request parameter data and DB query result data
- Track the processing of collected eternal data within WAS
- Record issues and block requests if threats are detected while tracing.

Efficient management

- Easily manage and change self protection policies and details
- View information and trends related to all attacks attempts detected by RASP
- Enable integrated management of multiple web applications

Reduce cost and required resource

- Quickly and flexibly defend against vulnerabilities without developing new programs
- Reduce new development costs by enabling vulnerability defense without developing new legacy systems
- Enable unified management of multiple web application security issues

Sparrow World Cup Buk-Ro, 6th Fl. Mapo-Gu, Seoul, 03925, Korea. Tel. 82-2-300-9232 Fax. 82-2-300-9200 Email: sparrow@fasoo.com

Sparrow RASP

Web application self protection solution that can detect and defend attacks by external input data in real time

System Requirements

RASP Console

OS

- Windows Server 2000 or later
- Ubuntu Linux 8.04 or later
- Redhat Linux 5 or later
- Fedora 8 or later
- CentOS or later
- JRE 1.7 or later

RASP Agent

- JRE 1.6 or later

RASP Core

- Java / JRE 1.6 or later
  .NET Framework 4.0

Supported Environment

Java

WAS

- Tomcat
- Jetty
- Jboss AS
- Wildfly
- WebLogic
- WebSphere Liberty Profile
- JEUS and more

Web Framework

- Spring Framework

JDBC Driver

- Oracle
- MySQL
- SQL Server
- Postgre SQL
- Maria DB
- HyperSQL and more

DB Framework

- MyBatis(iBatis)
  Hibernate

.NET

- -CLR 4.0

Dashboard & Statistic

- Set and manage WAS by projects
- Define and apply self protection policies and checker groups by projects

Detect and block attacks

- Track all external input data that occurs during web application operation
- Trace all request parameter data and DB query result data
- Detect and block all security threats occurred while tracing data during WAS internal operation

Vulnerability management

- Detect, record and manage attacks to the web application's protected WAS operation as issues
- Integrated management of all WAS' issue information by projects
- Vulnerability detection history management

Self protection policy management

- Enable or disable active web application self protection
- Apply or change self protection rules during web application operation
- Apply custom protection rules in real time
- Set log policies and vulnerability detection policies
- Set redirect page for detected vulnerabilities

Integrated management of multiple web applications

- Unlike traditional approaches that managed security threats and responses individually, with RASP, manage security issues across multiple web applications integratively
- Minimum performance load which is hardly recognizable

Major vulnerabilities

- OS command injection
- SQL injection
- Xpath injection
- Location based access control system roundabouts
- Database backdoor
- Consistent XSS
- Inconsistent XSS
- Dom based XSS
- Unvalidated redirections
- Unvalidated file upload

Sparrow World Cup Buk-Ro, 6th Fl. Mapo-Gu, Seoul, 03925, Korea. Tel. 82-2-300-9232 Fax. 82-2-300-9200 Email: sparrow@fasoo.com