

Sparrow RASP

Smart & Secure DevSecOps

Sparrow RASP(Runtime Application Self-Protection)는

WAF와 달리 애플리케이션의 런타임 환경 자체를 사용하여 실시간으로 외부의 요청과 내부의 응답을 모니터링합니다. 또한 더 정확한 보안 위협을 특정하여 경고를 표시하고 사이버 공격을 차단하거나 침해를 방지하기 위해 애플리케이션을 패치하여 자가방어를 구현할 수 있습니다.



포괄적인
WAS 지원



실용적인
관리 옵션



간단한
프로세스



스마트
도구

Sparrow RASP는 Tomcat, Jetty, JBoss AS, Wildfly, WebLogic, WebSphere Liberty Profile, JEUS 등 다양한 WAS(Web Application Server)에서 Java, .NET, PHP, Javascript 기반 애플리케이션을 지원합니다.

Sparrow RASP를 통해 하나의 서비스를 구성하는 복수의 애플리케이션을 관리하고 통합할 수 있습니다. 또한, 웹 브라우저에서 활성화 또는 비활성화 버튼을 사용하여 애플리케이션 방어 설정을 간단하게 제어할 수 있습니다.

Sparrow RASP는 실행 중인 웹 애플리케이션을 변경하지 않고 간단하게 설치할 수 있습니다. 오버헤드를 발생시키지 않도록 애플리케이션의 성능에 미치는 영향도 최소한으로 제한합니다.

Sparrow RASP는 애플리케이션에 대한 예상하지 못한 공격이나 익스플로잇을 모니터링하여 이에 대응하는 방법을 스스로 결정하는 스마트한 도구입니다.

지원 환경

OS

Windows Server 2000 이상,
Redhat Linux 5 이상, CentOS 5 이상,
Ubuntu 8.04 이상, Fedora 8 이상

WAS

Tomcat, Jetty, JBoss AS, Wildfly,
WebLogic, WebSphere Liberty
Profile, JEUS, 그 외 다수

프레임워크

Java 계열: Spring Framework,
iBATIS, MyBatis, Hibernate
C# 계열: ASP.NET MVC

JDBC 드라이버

Oracle, MySQL, SQL Server,
PostgreSQL, MariaDB, HyperSQL
그 외 다수

언어

. Java, .NET, Javascript, PHP

시스템 요구 사항

서버	
CPU	Quad Core 2.5GHz 이상
RAM	16GB 이상
HDD	300GB 이상

주요 체커

운영체제 명령어 삽입
SQL 삽입
XPath 삽입
제한되지 않은 파일 업로드
데이터베이스 백door
지속적 크로스사이트 스크립트
비지속적 크로스사이트 스크립트
DOM 기반 크로스사이트 스크립트
허용되지 않은 리다이렉션
경로 기반 접근 제어 시스템 우회



추가적인 애플리케이션 변경 없이 설치

- Java 기반 애플리케이션 지원
- .NET, PHP



한 번 클릭으로 보호 프로세스 활성화 및 비활성화



런타임 애플리케이션 보안 모니터링

- 삽입 공격 및 XSS 공격을 비롯한 테스트 규칙, 패턴



실시간으로 공격으로부터 웹 애플리케이션 보호

- 동시에 다수의 애플리케이션 보호 가능



5가지 위협도로 공격 구분



결과 보고서 생성

- 사용자 지정 보고서 지원 (PDF, Excel, Word, HTML, CSV)

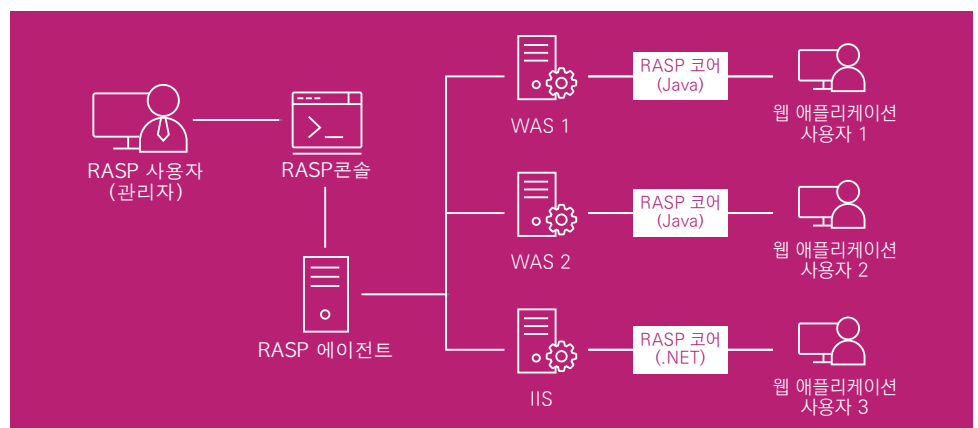
스파로우 보안·품질 솔루션 패키지

Sparrow **SAST/SAQT**

Sparrow **DAST**

Sparrow **SCA**

Sparrow **IHUB**



About Us

(주)스파로우는 2007년 파수닷컴의 사업부에서 시작하여 다년간의 경험을 바탕으로 소프트웨어의 품질과 보안을 책임지는 전문 기업입니다. 당사의 독자적인 기술을 바탕으로 국내 시장 점유율 1위의 시큐어코딩 도구인 Sparrow SAST/SAQT, 웹 취약점 분석 도구인 Sparrow DAST, 오픈소스 관리 도구인 Sparrow SCA, DevSecOps 관리 도구 Sparrow IHUB 등 SDLC 전반에 걸쳐 DevSecOps를 구현할 수 있도록 기여하고 있습니다.