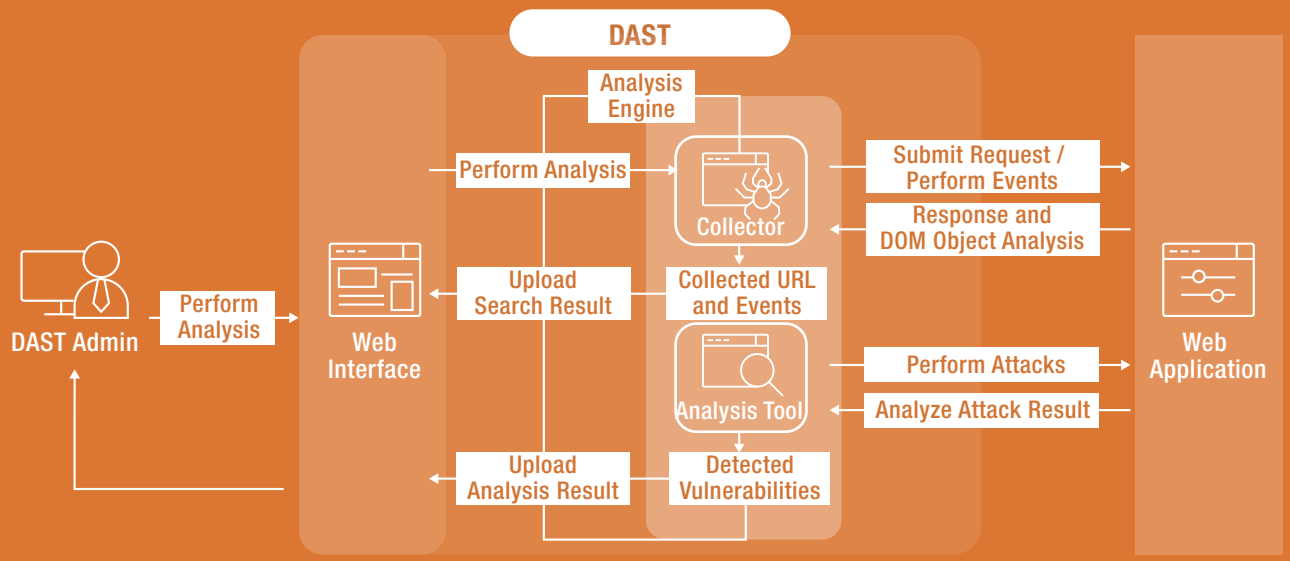
Sparrow DAST

Web application vulnerability dynamic analysis tool that provides powerful analysis capabilities and high usability



High Usability

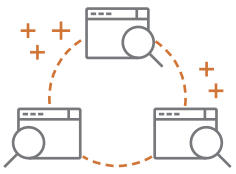
- No installation required!
- Run analysis with web based UI
- Concurrent scanning
- Easy to manage analysis results

Latest web application technology analysis

- Analyze web application that use latest technologies including HTML5 and AJAX

Powerful analysis

- Detect security vulnerabilities in web application using browser event replay technology



Interaction support

- Overcome limitations of dynamic analysis via interaction with other testing tools

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 DAST

Web application vulnerability dynamic analysis tool that provides powerful analysis capabilities and high usability

System Requirements

- **CPU:** Quad Core 2.5 GHz or faster
- **RAM:** 16GB or greater
- **HDD:** 300GB or larger

Supported Environment

Server

OS

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

DB

- Postgre SQL(embedded)

Automated detection of security vulnerability in web application

- Automatically collect sub directory information and URL of the web application with Sparrow Crawler
- Detect security vulnerabilities of collected directories

Support various types of web application analysis

- Support analysis of basic HTML message to latest AJAX
- Detect security vulnerabilities by reproducing various events that can be performed in the browser

Web based user interface

- Ability to perform and view results using a web browser
- Ability to overview security vulnerabilities trends in web application via dashboard

Multi-user optimized system

- Set roles and permission by users or groups
- Enable central management and sharing of analysis results

Analysis Reports

- Easy to read reports with clear vulnerability information and trends
- Detailed reports with analysis methods, results, and solution for each vulnerability

Major Checkers

- ☐ Reliance on DNS Lookups in a security decision
- ☐ HTTP response splitting
- ☐ LDAP injection
- ☐ SQL injection
- ☐ Xpath injection
- ☐ Path traversal / resource injection
- ☐ Improper authentication
- ☐ Missing or improper restriction of excessive authentication attempts
- ☐ Information exposure through persistent cookie
- ☐ System data information exposure
- ☐ URL direction to untrusted site
- ☐ Information exposure through an error message
- ☐ OS Command injection
- ☐ Malicious file upload
- ☐ Exposure of data element to wrong session
- ☐ Insecure/improper random number usage
- ☐ Missing authentication for critical function
- ☐ Integer overflow
- ☐ Leftover debug code
- ☐ Information exposure through comments
- ☐ Clear text storage of sensitive information
- ☐ Clear text transmission of sensitive information
- ☐ Incorrect permission assignment for critical resource
- ☐ Improper key length usage
- ☐ Usage of vulnerable API
- ☐ Weak password requirements
- ☐ Cross site scripting
- ☐ Cross site request forgery
- ☐ Format string injection

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