ZeroDay

AIAST

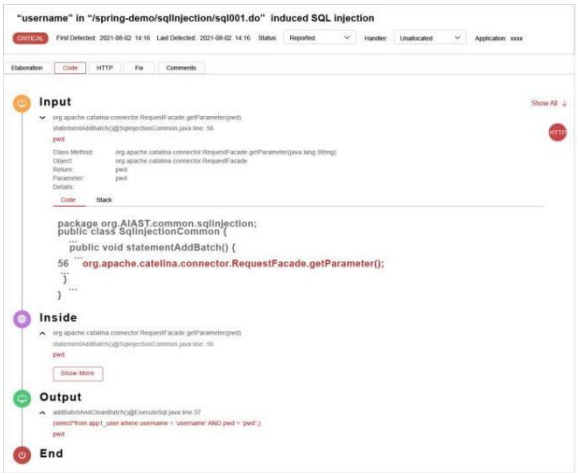
Advanced Interactive Application Security Testing

Overview

As the pioneering application security testing product of ZeroDay, AIAST is a tool that could enormously cut down the workload of developers and the investment of security professionals during the application development process. Meanwhile, it pinpoints the exact location of the vulnerabilities in the code and shows their detailed description and fix guidance with high accuracy and a low false positive rate.

Instrumentation-based Test

By taking advantage of instrumentation technology in the platform where the target application runs, it can record and display all the HTTP information of the application, track sensitive data flow, trace the stacks, and pinpoint the code lines where the vulnerabilities locate.

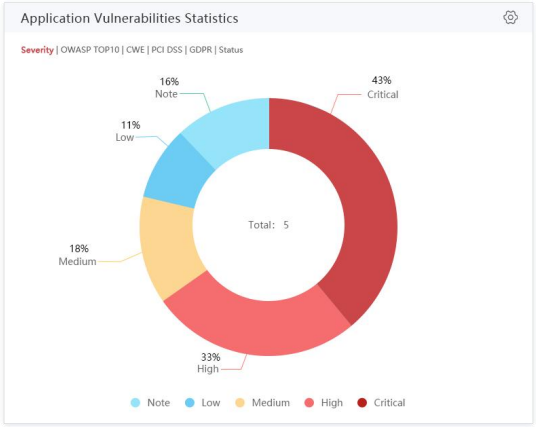


Automatic Test Process

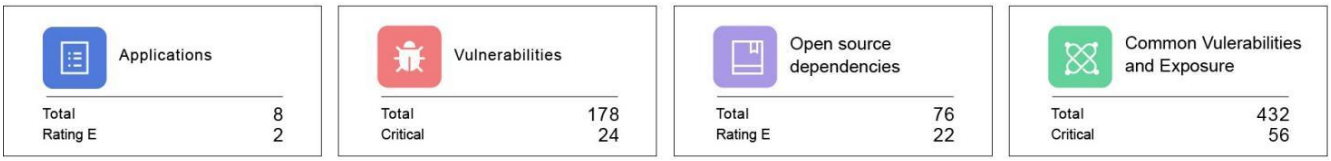
The test automatically takes place during the regular functional test, and the vulnerabilities will pop out spontaneously without any manual work. It frees the development and the DevOps team from spending extra time on security testing.

Broad Vulnerability Detection and Assessment

AIAST can detect all sorts of vulnerabilities publicly known by the industry and novel vulnerabilities discovered by our distinguished security experts. It adopts industry compliance standards including OWASP Top10, CWE, and CVE. Furthermore, it tracks sensitive data and locates risks in lines of code against data protection regulations such as PCI-DSS and GDPR.



Comprehensive application security posture



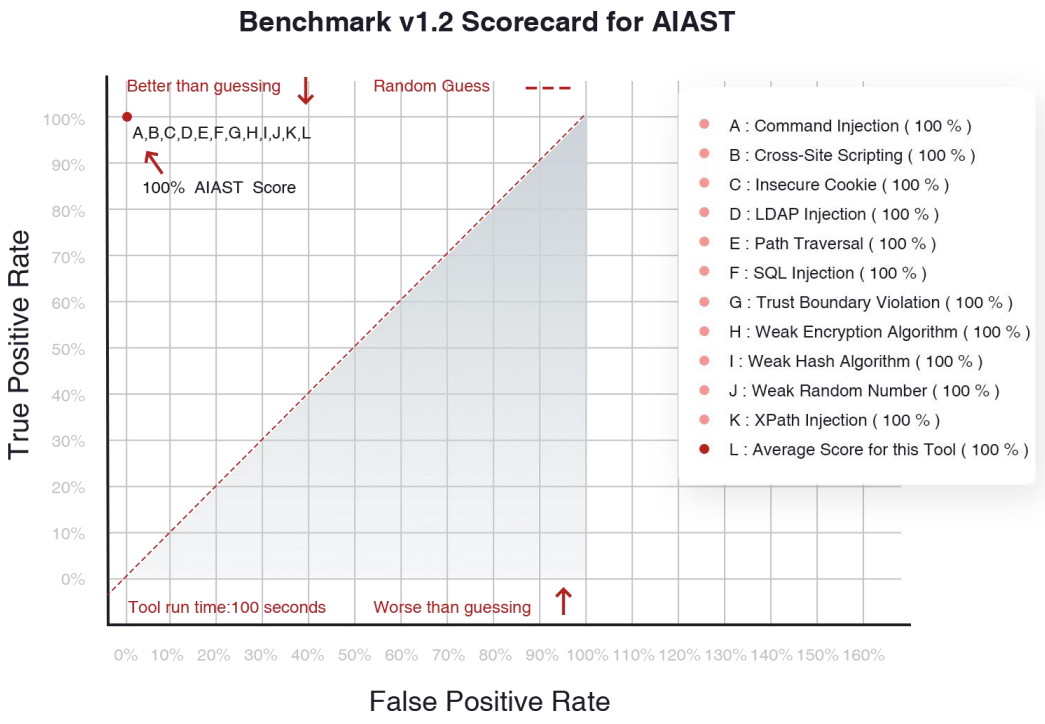
For the first time in the industry, the interactive application security testing tool seamlessly integrates the detection and analysis of all the open-source dependencies involved in the application. It reveals a comprehensive risk overview of the application, whose risk rating depends on the lower one comparing the risk of custom code with the open-source dependencies.

High accuracy and low false-positive rate

The AIAST adopts a series of measures to boost accuracy and reduce the false-positive rate.

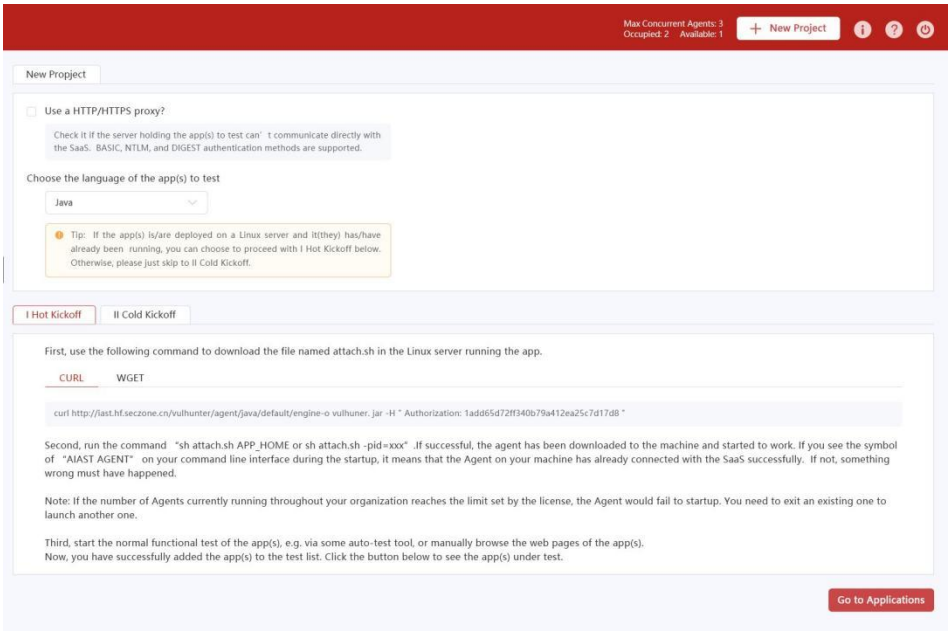
- Users can define custom rules against sanitizer, input validator, regular expression, and class filter. They may use custom rules for input validation or other processing to suppress certain types of vulnerabilities so that those vulnerabilities would not be reported in selected applications.
- Token/Key whitelist

- Users can customize regular expressions to track certain types of sensitive data and report vulnerabilities related to their exposure.
- Vulnerability Automatic Verification: Upon detection of certain types of potential vulnerabilities, AIAST can fabricate payloads to send to the URLs to confirm the validity of the vulnerabilities. After being verified, the vulnerabilities would have a verified icon next to their names in the vulnerabilities list.



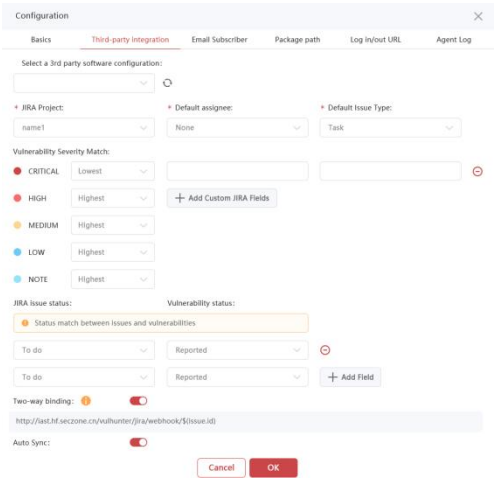
Ready to go & Quick start

- With the SaaS-based solution, no need to set up a server or install a bunch of software. It also saves your IT professionals time commissioning or maintaining your premise. It takes just any web browser and goes..
- With just a few steps, you can download the Agent on your application' s web server and start a new test.
- User-friendly interface, intuitive workflow, abundant and concise elaboration of technical terms, and various dashboards, enable any users with basic security knowledge to complete complex security test tasks with ease.



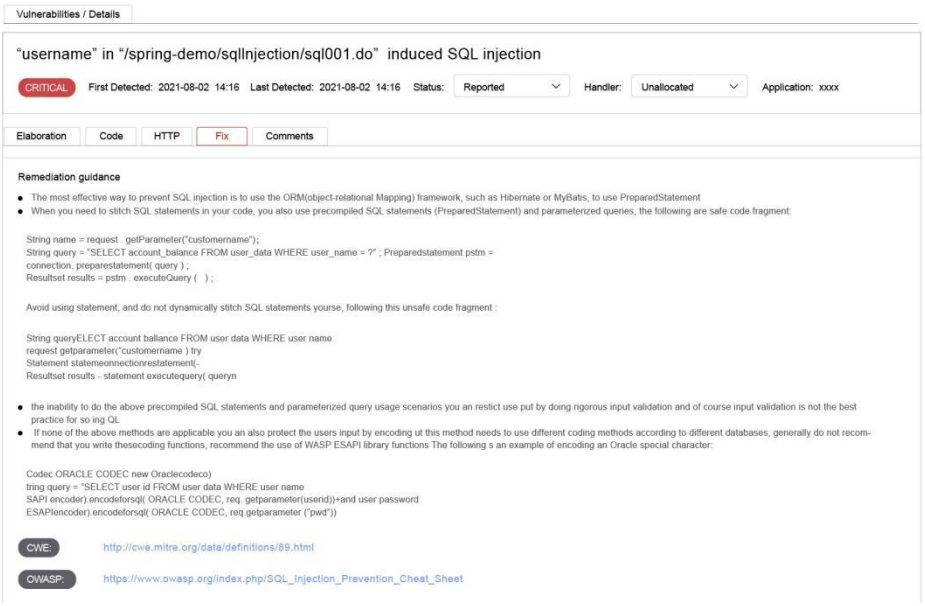
Seamless integration with DevOps tools

- Synchronization with Jira so that vulnerabilities detected in the AIAST can be sent to a configured Jira project and there is a status match between Jira issues and AIAST vulnerabilities.
- An AIAST plug-in can be uploaded to Jenkins to configure an automatic security test after build.
- Provide REST API for other services to get test data from AIAST, e.g., application info, vulnerabilities, open-source dependencies, test report, etc.



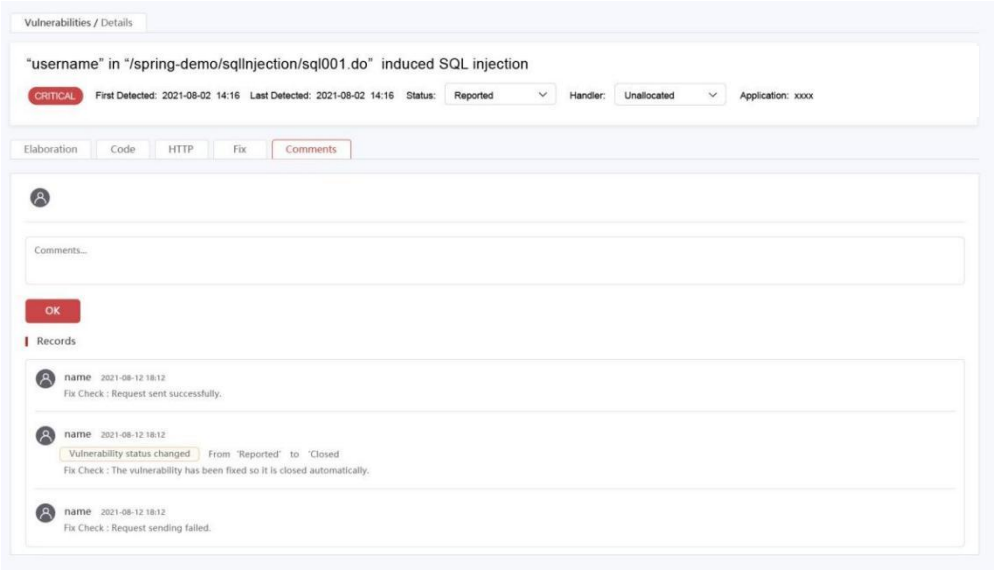
Detailed and customizable remediation guidance

There is corresponding remediation guidance detailing the specific measures or suggestions to undertake the detected vulnerability, along with code examples. Moreover, users can customize the remediation guidance for each type of vulnerability.



Fix check

- There is an "Automatic Fix Check" option in the application configuration. When selected, for those vulnerabilities in the application which support automatic fix check, AIAST would automatically resend payloads every few minutes to the specified URLs where the vulnerabilities were detected to check whether they have been fixed or not.
- There is also a Fix Check option in the application lists. Upon click, the AIAST would resend payloads to the specified URLs where the vulnerabilities (fix-checkable) locate to check whether they have been remediated or not. And such requests would be recorded in the comments section of the vulnerability details page.



AIAST | Technical Specifications

Supported language

Java

Node.js

C#/.NET

PHP

Python

Supported platform

Windows

Linux

MacOS

Unix like

Supported web server/application framework

Java

- Tomcat
- WebLogic
- Spring Boot
- Jetty
- WebSphere
- JBoss
- WildFly
- Resin
- WebSphere Liberty

Node.js

- Express

.Net

- .NET Framework

.PHP

- Nginx
- Apache

About ZeroDay

Founded in 2016, ZeroDay aims to make software development more secure and application security work simpler, saving your precious time and workforce.
Spearheaded by AIAST, our product portfolio will include software component analysis, static application security testing, dynamic application security testing, fuzz testing, and more in the coming days.

For more information about ZeroDay, visit us online at www.zeroday.co.uk

160 The Edge, Clowes Street Salford, Manchester, M3 5NE
U.K.

Sales: + 44-16-1350-8028