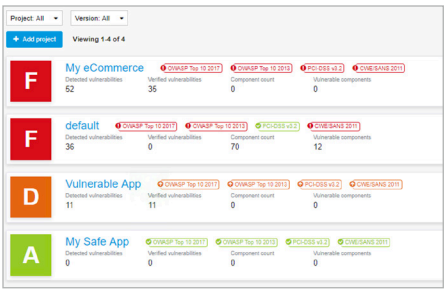
SYNOPSYS®

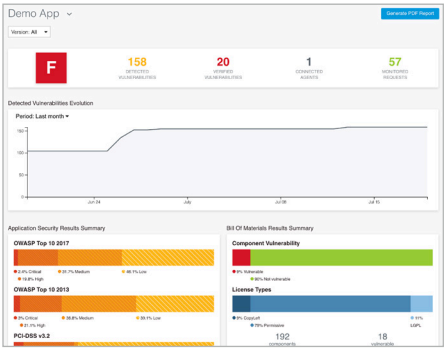
Seeker

Interactive Application Security Testing

Easy-to-use enterprise-scale IAST that accurately identifies *and* verifies vulnerabilities



Project security grades based on security vulnerability status.



Comprehensive dashboard view of top security vulnerabilities.

Overview

Seeker by Synopsys, our interactive application security testing solution, gives you unparalleled visibility into your web app security posture and identifies vulnerability trends against compliance standards (e.g., OWASP Top 10, PCI DSS, and CWE/SANS). Seeker enables security teams to identify and track sensitive data to ensure that it is handled securely and not stored in log files or databases with weak or no encryption. Seeker's seamless integration into CI/CD workflows enables fast IAST security testing at DevOps speed.

Unlike other IAST solutions, which only identify security vulnerabilities, Seeker can also determine whether a security vulnerability (e.g., XSS or SQL injection) can be exploited, thus providing developers with a risk-prioritized list of verified vulnerabilities to fix in their code immediately. Using patented methods, Seeker quickly processes hundreds of thousands of HTTP(S) requests, identifies vulnerabilities, and reduces false positives to near zero. This enables security teams to focus on actual verified security vulnerabilities first, greatly improving productivity and reducing business risk. It's like having a team of automated pen testers assessing your web applications 24-7.

Seeker applies code instrumentation techniques (agents) inside running applications and can scale to address large enterprise security requirements. It provides accurate results out of the box and doesn't require extensive, lengthy configuration. With Seeker, your developers don't have to be security experts, because Seeker provides detailed vulnerability descriptions, actionable remediation advice, and stack trace information and identifies vulnerable lines of code.

Seeker continuously monitors any type of testing applied to web apps and seamlessly integrates with automated CI build servers and test tools. Seeker leverages these tests (e.g., manual QA of log-in pages or automated functional tests) to automatically generate multiple security tests.

Seeker also includes Black Duck Binary Analysis, our software composition analysis (SCA) solution, which identifies third-party and open source components, known vulnerabilities, license types, and other potential risk issues. Seeker and Black Duck analysis results are presented in a unified view and can be sent directly to Jira, so developers can triage them as part of their normal workflow.

Seeker is ideal for microservices-based app development as it can bind together multiple microservices from a single app for assessment.

Continuous quick, actionable results

Comprehensive analysis results contain all the information necessary to address vulnerabilities:

- A clear explanation of the risk
- Runtime memory values and context
- A technical description
- The vulnerable lines of code
- Relevant, context-based remediation instructions

Multiple detailed panes show the dataflow and the impact of malicious inserted parameters (e.g., dynamic SQL concatenation). The results also show whether identified vulnerabilities have been auto-verified as exploitable or eliminated as false positives.

Seeker also integrates Black Duck Binary Analysis:

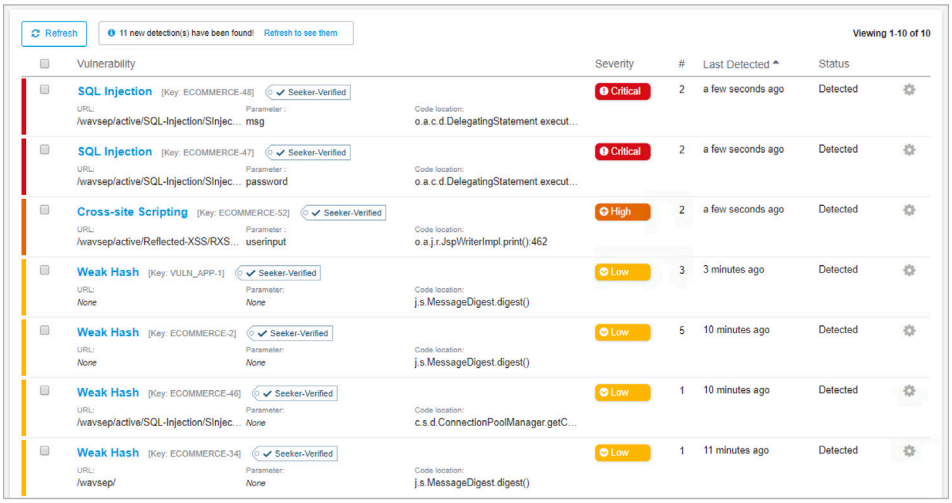
- Sends application binaries for SCA analysis and uploads the analysis results to the Seeker dashboard

Only enterprise-scale IAST solution with active verification

Seeker's unique active verification feature allows it to process hundreds of thousands of HTTP(S) requests and quickly eliminate false positives from identified vulnerabilities, for near-zero false positives. For enhanced test coverage, Seeker's parameter identification feature detects unused parameters and retests them using malicious values, thus exploring more potential application attack surfaces, hidden parameters, and back doors.

Benefits:

- Both security and development teams see greatly improved productivity.
- Lower overall costs / fewer resources are required for dynamic application security testing (DAST) or manual pen testing.



Easy to deploy and use

Seeker uses instrumentation techniques and runtime analysis to continuously monitor, identify, and verify security vulnerabilities in web applications, typically during the test/QA stage of the software development life cycle (SDLC). Applications can be on-premises, microservices-based, or cloud-based. Seeker supports modern app development methodologies and technologies. Simply deploy agents at each tier or node of an application that runs code (Docker containers, virtual machines, cloud instances, etc.), and they'll track every action performed on the running app. Analysis results are available right away, without the need for any special scans.

Not only does Seeker analyze code line by line, correlating dataflow and runtime code execution in real time; it also examines the interaction of the code with your sensitive data across all application tiers and components. This technology identifies vulnerabilities that pose a real threat to critical data, including complex vulnerabilities and logical flaws no other technology can detect.

Get started with Seeker right away

- **Fits seamlessly into CI/CD workflows.** Native integrations and web APIs provide seamless integration with the tools you use for on-premises, cloud-based, microservices-based, and container-based development.
- **Deploys quickly and easily.** Seeker provides real-time analysis with near-zero false positives, out of the box.
  - Accurate out of the box with no extensive configuration or tuning
  - No need for website log-in credentials or special scans
  - Active verification takes into account input validation libraries and custom functions to sanitize inputs (e.g., SQL injection vulnerabilities)
  - Scalable in large enterprise environments
- **Works with virtually any type of test method.** Seeker's nonobtrusive passive monitoring option allows it to work with existing automation tests, QA/dev tests, automated web crawlers, unit testing, etc.

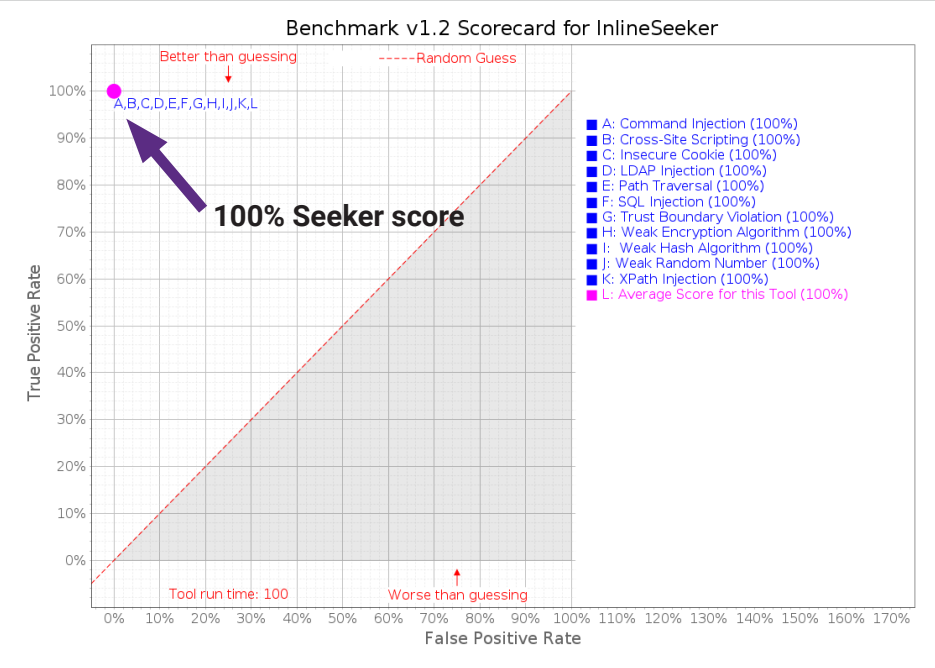
URL discovery and coverage of your web app

Automated URL mapping provides a clear view of the test coverage of a web app and graphically shows what has been already tested. You can easily compare coverage differences between different versions of the same app.

Sensitive-data tracking

Seeker's unique ability to track sensitive data is an industry first. Users can mark data as sensitive (e.g., credit card numbers, usernames, and passwords) so that these data can be tracked whenever they are stored unencrypted in a log, database, or file. Tracking sensitive data can help you achieve compliance with the sections of PCI DSS that require data encryption, as well as other industry standards and regulations such as GDPR. This enables substantial gains in productivity and time savings over manual inspection, as well as savings in costs and resources.

Highest OWASP Benchmark Score



SYNOPSYS®

Seeker
Technical Specifications

Supported languages

- ASP.NET
- C#
- Clojure
- Gosu
- Groovy
- Java
- JavaScript (Node.js)
- Scala (incl. Lift)
- VB.NET

Supported platforms

Languages/testing platforms

- Java
  - Any Java EE server
  - GlassFish
  - JBoss
  - Tomcat
  - WebLogic
  - WebSphere
- .NET (2.0 or higher)
  - IIS
- Node.js (6 or higher)
  - Express
  - Hapi
  - Koa

Runtime/frameworks

- .NET/CLR
  - ASP.NET MVC
  - Enterprise Library
  - Entity Framework
  - NHibernate
  - Ninject
  - NVelocity
  - OWASP ESAPI
  - SharePoint
  - Spring.NET
  - Telerik
  - Unity
- Java/JVM
  - Enterprise JavaBeans (EJB)
  - Grails
  - GWT
  - Hibernate
  - OWASP ESAPI
  - Play
  - Seam
  - Spring
  - Struts
  - Vaadin
  - Velocity

Technologies

- Databases
  - DB2
  - HSQLDB
  - MongoDB
  - MS SQL
  - MySQL
  - Oracle
  - PostgreSQL
- Application types
  - Ajax
  - JSON
  - Microservices
  - Mobile (over HTTP/S)
  - RESTful
  - Single-page applications
  - SOAP
  - Web (incl. HTML5)
  - Web APIs
  - Web services

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle.

For more information go to www.synopsys.com/software.

Synopsys, Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com