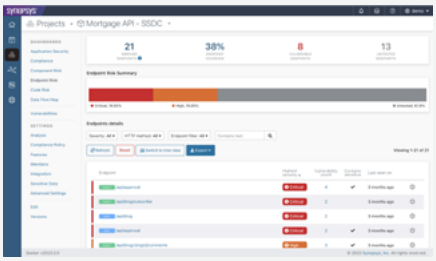
Seeker

Interactive Application Security Testing

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



Comprehensive dashboard view of top security vulnerabilities from application to components and APIs involved.

Instant visualization with detailed test coverage and data flow tracking. It displays the architecture of the system under test, including data flowing into the app from various sources, data flowing between different components of the system, and outgoing calls to third-party APIs and web services.

Overview

Seeker® Interactive Analysis, our interactive application security testing (IAST) 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, GDPR, CAPEC, and CWE/SANS Top 25). 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 DevOps CI/CD workflows enables continuous application security testing and verification.

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 it 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 login 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 automatically to bug-tracking and collaboration systems of choice, 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.

Seeker analyzes the flow of data between microservices to analyze the system as a whole, not just as a set of unrelated applications. Data flows are tracked over HTTP(S), gRPC, shared databases, and more.

Continuous quick, actionable results in real time

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.

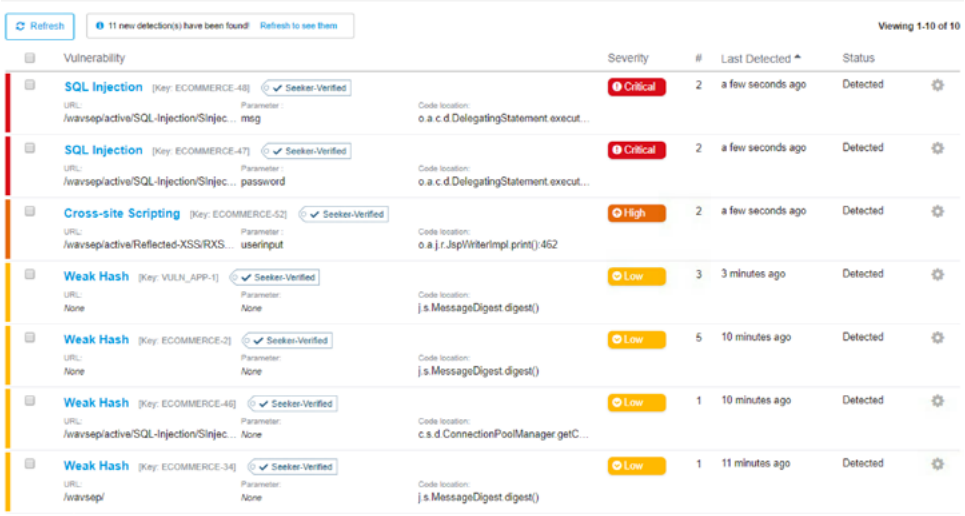
Seeker also integrates Black Duck Binary Analysis and SCA, which sends application binaries for composition analysis and uploads the results to the Seeker dashboard.

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, helping to ensure 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 integration testing and QA, right up to the production deployment stage of the software development life cycle (SDLC). Applications can be on-premises, microservices-based, serverless functions 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 in real time, 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 microservices, and API calls across the 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.

Seeker's integration with eLearning and Secure Code Warrior provides contextual help and training for developers and DevOps teams. It allows them to gain in-depth understanding of vulnerabilities and remediate them easily and in real time.

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 login 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 test automation, manual or functional tests, automated web crawlers, and more.

Detailed test coverage with API discovery, tracking, and data flow map of your app and microservices

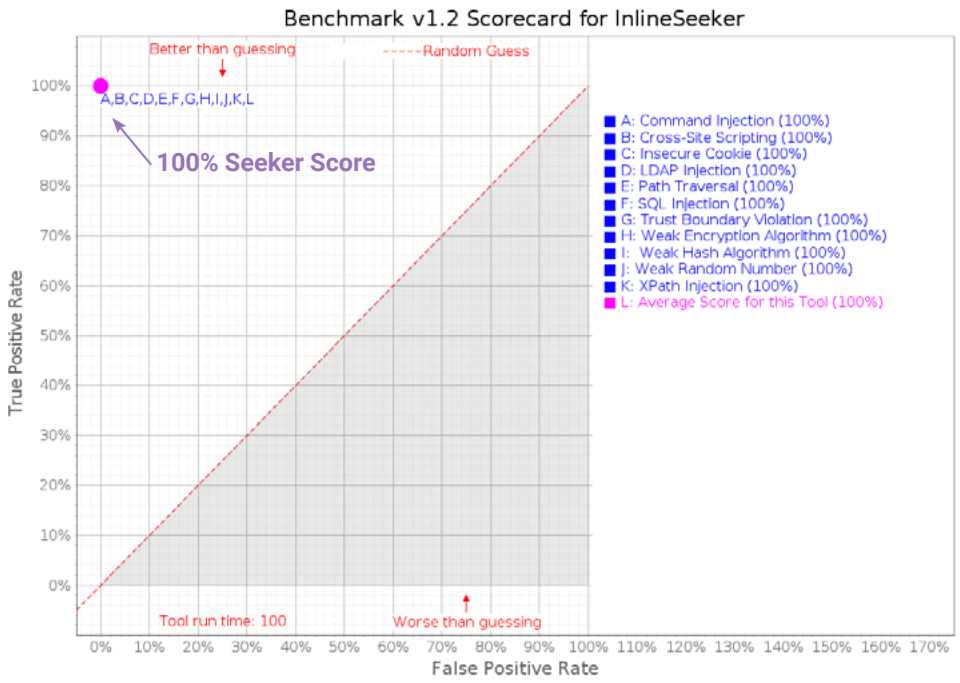
Automated URL mapping, API discovery, and endpoints tracking provides a comprehensive view of the extent of test coverage of a web app. Seeker graphically shows what has already been tested and what has not been tested, as well as provides visual data flow mapping that aids in effective taint analysis. You can easily compare coverage differences between different versions of the same app.

Active verification automatically generates sequences of requests to boost coverage for OpenAPI/Swagger and Graph-QL based applications.

Sensitive-data and secrets tracking

Seeker's unique ability to track sensitive data and secrets is an industry first. Users can mark data as sensitive (e.g., credit card numbers, tokens, and passwords) so that this data can be tracked whenever it is 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 compliance, 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



Seeker | Technical Specification

Supported languages
- ASP.NET
- C#
- Clojure
- ColdFusion
- Go
- Gosu
- Groovy
- Java
- JavaScript (Node.js)
- Kotlin
- PHP
- Python
- Scala (incl. Lift)
- VB.NET

Supported platforms
- Java
  - Any Java EE server
  - GlassFish
  - Red Hat JBoss Enterprise Application Platform
  - Red Hat JBoss Web Server
  - Tomcat
  - WebLogic
  - WebSphere
- .NET Framework
  - IIS
  - WCF
  - OWIN
  - SharePoint
- .NET Core
- Node.js
- PHP

Runtime/frameworks
- .NET/CLR
  - ASP.NET MVC
  - Enterprise Library
  - Entity Framework
  - NHibernate
  - Ninject
  - NVelocity
  - OWASP ESAPI
  - SharePoint
  - Spring.NET
  - Telerik
  - Unity
- GO
  - Chi
  - Echo
  - Gin
  - Net/http
- Java/JVM
  - Enterprise JavaBeans (EJB)
  - Grails
  - GWT
  - Hibernate
  - Ktor
  - Micronaut
  - OWASP ESAPI
  - Play
  - Ring
  - Seam
  - Spring/Spring Boot
  - Struts
  - Vaadin
  - Velocity
  - Vert.x
- Java Runtime:
  - AdoptOpenJDK
  - Amazon Corretto
  - Eclipse OpenJ9
  - IBM
  - Oracle HotSpot
  - OpenJDK
  - Red Hat OpenJDK
- Node.js
  - Express
  - Fastify
  - Hapi
  - Koa
- PHP
  - Laravel
  - Symfony
- Python
  - Django
  - Flask

Technologies
- Databases
  - NoSQL DB
    - Cassandra
    - Couchbase
    - DynamoDB
    - HBase
    - MongoDB
- Relational/SQL
  - DB2
  - HSQLDB
  - MS SQL
  - MySQL
  - PostgreSQL
  - SQLite
  - Oracle
- Application types
  - Ajax
  - JSON
  - Microservices
  - Mobile (over HTTP/S)
  - RESTful
  - Single-page applications
  - Web (incl. HTML5)
  - Web APIs
  - Web services
- Interprocess communications
  - HTTP(S)
  - gRPC
  - Kafka
  - Apache Dubbo
  - RabbitMQ
  - JMS
  - Database tables

Cloud platforms
- Azure PaaS/Azure Function
- AWS
- AWS Lambda
- Google Cloud
- Tanzu (PCF)

phase pacific

Need Local Support?

Contact: Frank Cappellari
Email: frank.cappellari@phasepacific.com
Mobile: +61 449 205 670
Office: +61 (03) 9381 7818

About Black Duck

Black Duck® offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.

©2024 Black Duck Software, Inc. All rights reserved. Black Duck is a trademark of Black Duck Software, Inc. in the United States and other countries. All other names mentioned herein are trademarks or registered trademarks of their respective owners. August 2024