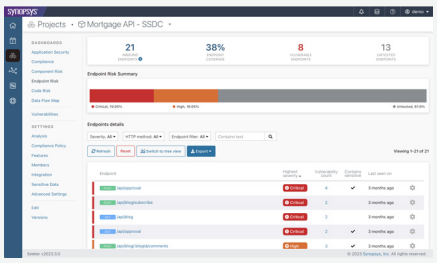
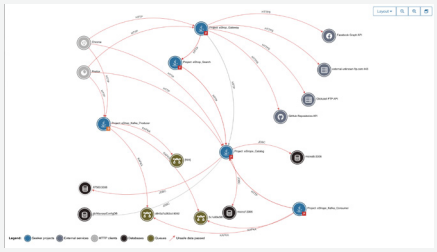
Seeker® Interactive Analysis

대화형 애플리케이션 보안 테스트 도구

취약점을 간단하고
정확하게 식별 및
검증하는 사용하기 쉬운
엔터프라이즈용 IAST



애플리케이션, 컴포넌트, API 등의 보안 취약점을 한눈에 파악할 수 있는 통합 대시보드.



빠른 시각화, 폭넓은 테스트 범위, 데이터 흐름 추적 기능. 다양한 소스에서 앱으로 이동하는 데이터, 여러 컴포넌트 사이에서 이동하는 데이터, 3자 API 및 웹 서비스 호출 정보 등 테스트 시스템의 아키텍처를 표시합니다.

개요

Seeker®는 Black Duck®의 대화형 애플리케이션 보안 테스트(IAST) 솔루션입니다. 웹 애플리케이션 보안 태세에 대한 탁월한 가시성을 제공하며, 보안 표준을 바탕으로(예: OWASP Top 10, PCI DSS, GDPR, CAPEC 및 CWE/SANS Top 25) 취약점 추이를 파악합니다. Seeker를 통해 민감한 데이터를 식별 및 추적하여 데이터를 안전하게 보호하고, 암호화가 되어 있지 않은 상태로 로그 파일이나 데이터베이스에 데이터가 저장되지 않도록 관리할 수 있습니다. Seeker는 DevOps CI/CD 워크플로에 원활하게 통합됩니다. 따라서 애플리케이션 보안 테스트 및 검증을 지속적으로 수행할 수 있습니다.

보안 취약점 식별에 그치는 여타 IAST 솔루션과 달리 Seeker는 보안 취약점(예: XSS 또는 SQL 주입)의 악용 가능성을 판단하고, 위험도를 평가하고 확인된 취약점 리스트를 제공하여 개발자가 즉시 코드를 수정할 수 있도록 해줍니다. Seeker는 특허 기술을 바탕으로 수십만 개의 HTTP(S) 요청을 빠르게 처리하고, 취약점을 식별하며, 오탐률을 제로 수준으로 줄입니다. 이제 보안팀은 확인된 보안 취약점에 집중할 수 있습니다. 생산성은 크게 향상되고, 비즈니스 위험은 대폭 줄어듭니다. 마치 자동화된 침투테스트 팀이 웹 애플리케이션을 연중무휴 24시간 평가해 주는 것과 같습니다.

Seeker는 실행 애플리케이션에 코드 인스트루멘테이션 기법(에이전트 기반)을 적용하며, 대규모 기업의 수많은 보안 요구 사항에 유연하게 대응할 수 있습니다. Seeker는 빠르고 정확한 결과를 제공하며, 구성이 복잡하거나 번거롭지 않습니다. Seeker는 취약점 상세 정보, 유용한 수정 제안, 스택 추적 정보 등을 제공하고, 취약한 코드 라인 위치까지 식별해 주기 때문에 보안 전문가가 아니더라도 얼마든지 활용 가능합니다.

Seeker는 웹 애플리케이션에 적용되는 모든 유형의 테스트를 지속적으로 모니터링하고, 자동화된 CI 빌드 서버 및 테스트 도구와 원활하게 통합됩니다. Seeker는 이러한 시스템(예: 로그인 페이지의 수동 QA 테스트 또는 자동화된 기능 테스트)을 활용하여 여러 가지 보안 테스트를 자동으로 실행합니다.

또한, 소프트웨어 구성 분석(SCA) 솔루션인 Black Duck SCA Binary Analysis가 Seeker에 포함되어 있어, 오픈 소스의 구성요소, 알려진 취약점, 라이선스 유형, 기타 잠재적 위험 등을 식별합니다. 이후 Seeker와 Black Duck 분석 결과를 한꺼번에 표시하고, 원하는 협업 시스템 및 버그 추적 시스템에 자동으로 보냅니다. 개발자는 이를 기존 워크플로와 동일하게 처리할 수 있습니다.

Seeker는 단일 애플리케이션에 여러 마이크로서비스를 묶어서 같이 평가할 수 있으므로 마이크로서비스 기반 애플리케이션 개발에 제격입니다.

Seeker는 마이크로서비스 간의 데이터 흐름을 파악하여 개별 애플리케이션뿐만 아니라 시스템 전체를 분석합니다. HTTP(S), gRPC, 공유 데이터베이스 등에서 데이터 흐름을 추적합니다.

빠르고 유용한 실시간 분석 결과

종합 분석 결과는 다음과 같은 취약점 해결에 필요한 모든 정보가 포함됩니다.

- 위험에 대한 명확한 설명
- 런타임 메모리값 및 컨텍스트
- 기술적 설명
- 취약한 코드 라인
- 컨텍스트 기반의 효과적 수정 지침

여러 개의 상세 정보 창을 통해, 악의적으로 삽입된 매개변수(예: 동적 SQL 연결)의 영향과 데이터 흐름을 보여줍니다. 또한, 식별된 내용 중 어느 것이 오탐이고 어느 것이 악용 가능한 것인지 자동으로 확인합니다.

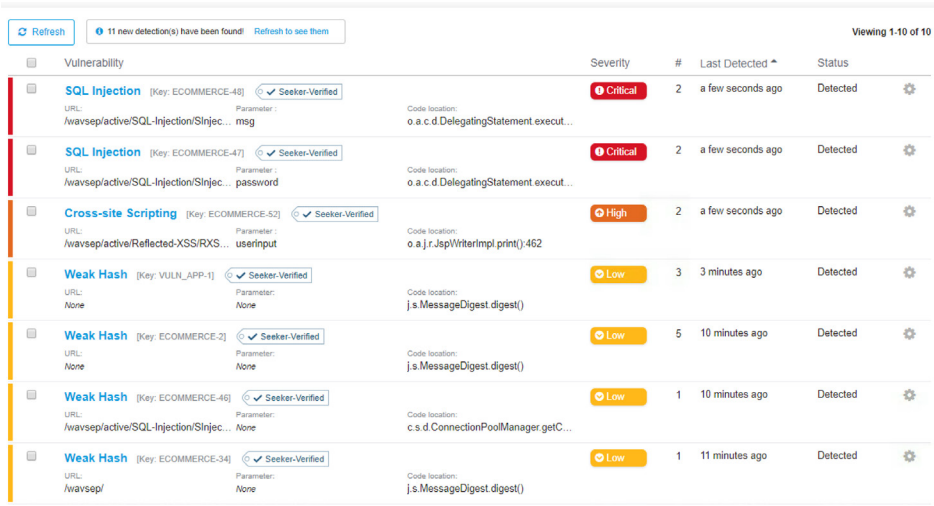
Seeker에 통합 가능한 Black Duck Binary Analysis와 SCA는 애플리케이션 바이너리의 구성 분석을 지원하고 Seeker 대시보드에 결과를 업로드합니다.

능동 검증을 지원하는 엔터프라이즈용 IAST 솔루션

Seeker만의 능동 검증 기능으로 수십만 개의 HTTP(S) 요청을 처리하고, 식별된 취약점 가운데 오탐을 신속하게 제거하여, 오탐률을 제로 수준으로 유지합니다. Seeker의 매개변수 식별 기능은 미사용 매개변수를 분석하고, 악성 값을 새로 테스트하여, 애플리케이션 공격 경로, 숨은 매개변수, 백도어 등을 더욱 폭넓게 탐색합니다.

장점

- 보안팀과 개발팀의 생산성이 크게 향상됩니다.
- 동적 애플리케이션 보안 테스트(DAST) 또는 수동 침투테스트에 필요한 비용 및 리소스가 절약됩니다.



쉬운 설치 및 사용

Seeker는 인스트루멘테이션 기법 및 런타임 분석을 사용하여 웹 애플리케이션의 보안 취약점을 지속적으로 모니터링, 식별, 검증합니다. 이러한 동작은 QA 테스트 단계에서부터 소프트웨어 개발 수명주기(SDLC)의 프로덕션 배포 단계까지 지속됩니다. 이는 온프레미스 애플리케이션, 마이크로서비스 기반 애플리케이션, 서버리스 기능 애플리케이션, 클라우드 기반 애플리케이션 등에 모두 적용됩니다. Seeker는 최신 애플리케이션 개발 방법 및 기술을 지원합니다. 코드가 실행되는 애플리케이션의 각 계층 또는 노드(Docker 컨테이너, 가상 머신, 클라우드 인스턴스 등)에 에이전트를 설치하기만 하면 애플리케이션의 모든 작업을 추적할 수 있습니다. 분석 결과는 별도의 스캔 과정 없이 실시간으로 확인할 수 있습니다.

Seeker는 데이터 흐름과 런타임 코드 실행을 실시간으로 확인하여 코드를 빠짐없이 분석합니다. 또한, 모든 애플리케이션 계층 및 구성 요소에서 민감한 데이터와 코드 사이의 상호 작용을 검사합니다. 이 기술은 주요 데이터에 실제 위협이 되는 취약점(다른 기술로는 감지 불가능한 복잡한 취약점과 논리적 결함 등)을 식별합니다.

또한, Seeker에 통합된 e-러닝(유료) 및 Secure Code Warrior는 상황별 도움말과 교육을 제공하여 개발자와 DevOps 팀이 취약점에 대해 정확히 이해하고 실시간으로 해결할 수 있도록 지원합니다.

지금 바로 Seeker를 사용해 보세요

- **CI/CD 워크플로에 완벽 통합 -** 기본 통합 및 웹 API로 온프레미스, 클라우드 기반, 마이크로서비스 기반, 컨테이너 기반 개발에 사용하는 도구와의 원활한 통합을 지원합니다.
- **쉽고 빠른 배포 -** Seeker는 실시간 분석을 기본 제공하며, 오탐률은 제로에 가깝습니다.
  - 복잡하고 번거로운 구성 및 조정이 필요 없는 정확성
  - 별도의 스캔이나 웹사이트 로그인 자격 증명 불필요
  - 능동적 검증은 입력값 검사 라이브러리 및 사용자 지정 함수를 통해 입력 오류를 제거 (예: SQL injection)
  - 대규모 엔터프라이즈 환경에 맞게 확장 가능
- **모든 유형의 테스트 체계 지원 -** Seeker는 비간섭적 수동 모니터링 옵션을 이용해 기존 테스트 자동화, 수동/기능 테스트, 자동화 웹 크롤러 등과 호환됩니다.

애플리케이션과 마이크로서비스에 대한 API 탐색, 추적, 데이터 흐름 맵으로 폭넓은 테스트 범위

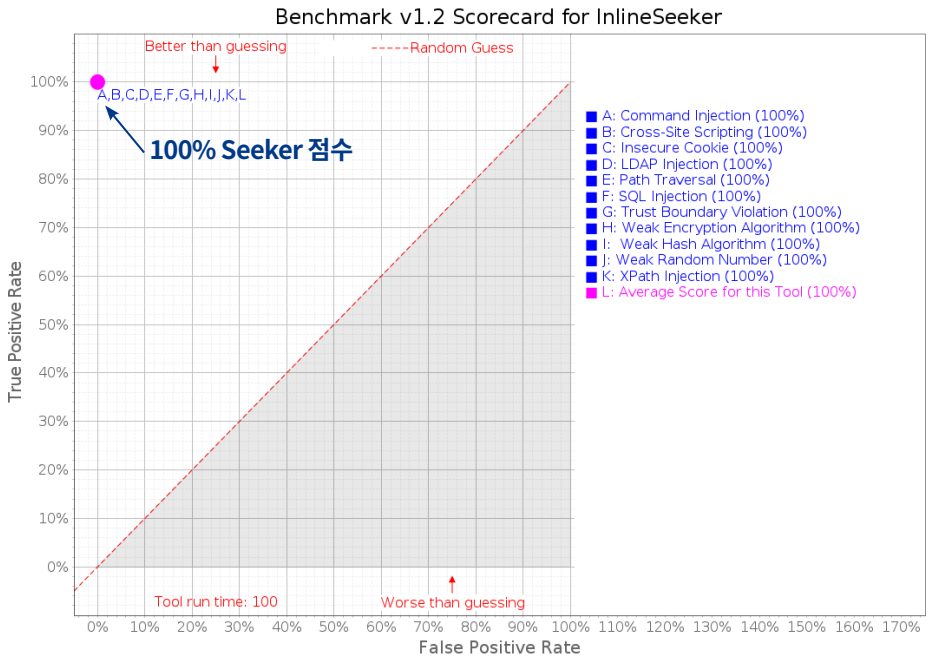
자동 URL 매핑, API 탐색, 엔드포인트 추적으로 웹 애플리케이션에 대한 테스트 범위를 한눈에 파악할 수 있습니다. Seeker는 무엇이 테스트를 마쳤고 무엇이 아직 테스트를 마치지 않았는지 일목요연하게 정리해서 보여줄 뿐 아니라, 오염 분석을 지원하는 데이터 흐름 맵을 제공합니다. 애플리케이션 버전 간 테스트 범위도 간편하게 비교할 수 있습니다.

능동 검증 시스템을 통해 OpenAPI/Swagger 및 Graph-QL 기반 애플리케이션에 대한 테스트 범위를 넓히기 위한 요청 시퀀스를 자동으로 생성합니다.

민감한 데이터 및 시크릿 추적

Seeker는 업계 최초로 민감한 데이터를 추적하는 기능을 제공합니다. 사용자가 민감한 데이터(예: 신용 카드 번호, 사용자 이름 및 암호)를 지정하면 민감한 데이터가 암호화되지 않은 상태로 로그, 데이터베이스, 또는 파일 등에 저장될 때마다 해당 데이터를 추적합니다. 민감한 데이터 추적은 데이터 암호화가 필요한 PCI DSS 섹션은 물론 GDPR과 같은 기타 산업 표준 및 규정을 준수하는 데도 도움이 됩니다. 이로써 생산성이 크게 향상되며, 시간, 비용, 자원을 대폭 절약할 수 있습니다.

OWASP 벤치마크 최고 점수



Seeker | 기술 사양

지원 언어

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

지원 플랫폼

- 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

런타임/프레임워크

- .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

기술

- 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

클라우드 플랫폼

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

Black Duck 소개

Black Duck®은 업계에서 가장 포괄적이고 강력하며 신뢰할 수 있는 애플리케이션 보안 솔루션 포트폴리오를 제공합니다. 전 세계 기업이 소프트웨어를 신속하게 보호하고, 개발 환경에 보안을 효율적으로 통합하며, 새로운 기술을 통해 안전하게 혁신할 수 있도록 지원하는 탁월한 실적을 보유하고 있습니다. 소프트웨어 보안 분야에서 인정받는 리더, 전문가, 혁신적인 기업인 Black Duck은 소프트웨어에 대한 신뢰를 구축하는 데 필요한 모든 것을 갖추고 있습니다.

자세한 내용은 www.blackduck.com 에서 알아보십시오.

©2024 Black Duck Software, Inc. All rights reserved. Black Duck은 미국 및 기타 국가에서 Black Duck Software, Inc의 상표입니다. 여기에 언급된 기타 명칭은 각 해당 업체의 등록 상표입니다. 2024년 10월