SYNOPSYS®

# Seeker
## 交互式应用安全测试

### 易于使用的企业级 IAST（交互式应用安全测试），能够准确地识别并验证漏洞

基于安全漏洞状态的项目安全等级。

顶级安全漏洞的综合仪表板视图。

## 概述

Seeker 是 Synopsys 公司提供的交互式应用安全测试解决方案，能够为您带来无与伦比的可视化的深入观察 Web 应用的安全状况并发现基于各种合规性标准（例如，OWASP Top 10、PCI DSS 和 CWE/SANS）的漏洞趋势。Seeker 能够让安全团队识别和跟踪敏感数据，以确保这些数据得到安全地处理，而且不会存储在弱加密或无加密的日志文件或数据库中。Seeker 与 CI/CD 工作流程无缝集成，可实现 DevOps 速度的快速 IAST 安全测试。

不同于其他仅识别安全漏洞的 IAST 解决方案，Seeker 还可以确定某个安全漏洞（例如，XSS 或 SQL 注入）是否被利用，从而为开发人员提供一份经过验证的漏洞风险优先级列表，以便立即修复其代码。借助于各种获得专利的方法，Seeker 能够快速处理数十万条 HTTP(S) 请求，能够识别出各种漏洞，并能够把误报数量降低至接近于零。这使得安全团队能够首先关注真正的、经过验证的安全漏洞，从而大大提高生产力并降低业务风险。这就像拥有一支渗透测试团队对您的 Web 应用进行 24x7 的评估。

Seeker 在运行的应用中采用代码 instrumentation 技术，并可以进行扩展以满足大型企业的安全要求。它能够开箱即用地提供精确结果，不需要大量、冗长的配置。采用 Seeker 时，您的开发人员不必是安全专家，因为 Seeker 提供了详细的漏洞描述、可操作的补救建议以及堆栈跟踪信息，并能够识别出易受攻击的代码行。

Seeker 能够持续监控用于 Web 应用的任何类型的测试，并能够无缝地与自动 CI 构建服务器及测试工具相集成。Seeker 利用这些测试（例如，登录页面的手动 QA 或者自动功能测试）来自动生成多种安全测试。

Seeker 中还包含黑鸭（Black Duck）二进制分析，这是我们的软件组成分析（SCA）解决方案，能够识别第三方和开源组件、已知漏洞、许可证类型以及其他潜在风险问题。Seeker 和黑鸭分析结果以统一视图显示，可以直接发送给 Jira，这样，开发人员就可以在他们的正常工作流程中对这些结果进行分类。

Seeker 非常适合基于微服务的应用开发，因为它可以将来自单个应用的多个微服务绑定在一起进行评估。

## 持续、快速、可操作的结果

综合分析结果包含了解决漏洞所需要的全部信息：

- 明确的风险解释
- 运行时内存值和上下文
- 技术说明
- 易受攻击的代码行
- 相关的、基于上下文的补救说明

多个详细窗格显示数据流和恶意插入的参数（例如，动态 SQL 连接）的影响。结果还显示是否已识别出的漏洞已被自动验证为可利用的或是作为误报而删除。

Seeker 还整合了黑鸭的二进制分析：

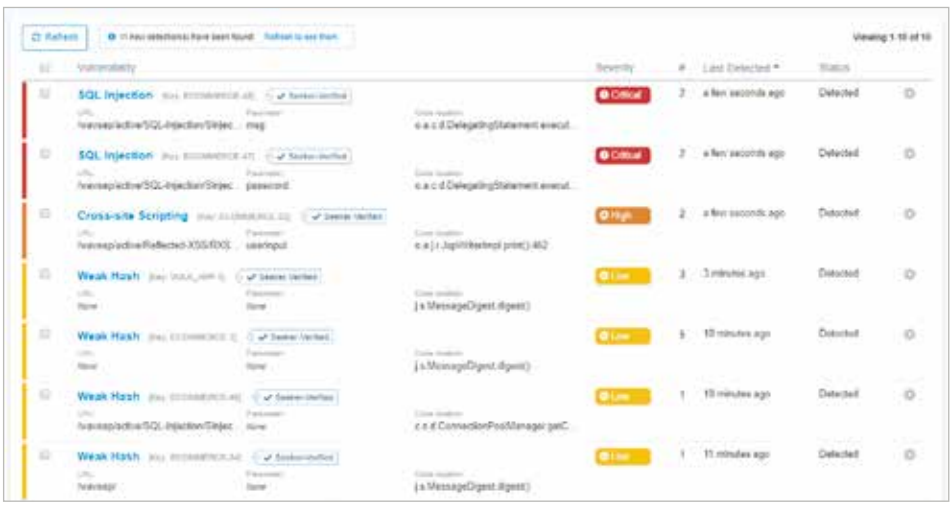
- 发送应用程序二进制文件进行 SCA 分析，并将分析结果上传到 Seeker 仪表板

## 唯一一款具有主动验证功能的企业级 IAST 解决方案

Seeker 独特的主动验证功能使其能够处理数百个千级 HTTP(S) 请求，并快速消除已识别漏洞的误报，从而实现接近于零的误报率。为了增强测试覆盖率，Seeker 的参数识别功能可以检测未使用的参数，并利用恶意值对它们进行重新测试，从而搜寻更多的潜在应用攻击面、隐藏的参数和后门。

优势：

- 安全团队和开发团队都能够大幅度提高生产力。
- 动态应用程序安全测试（DAST）或手动笔测试需要的总体成本更低 / 资源更少。




## 易于部署和使用

Seeker 利用 instrumentation 技术和运行时分析来持续地监控、识别和验证 Web 应用程序中的安全漏洞，通常在软件开发生命周期（SDLC）的测试 /QA 阶段完成。应用可以是内部部署的、基于微服务的或基于云计算的。Seeker 支持现代应用开发方法和技术。只需要在运行代码的应用的每个层或节点上（Docker 容器、虚拟机、云实例等）部署代理，它们就会跟踪在所运行的应用上执行的每个操作。分析结果可立即获得，无需进行任何特殊扫描。

Seeker 不仅能够逐行分析代码，并实时关联数据流和运行时代码执行；它还能够在所有应用程序层和组件中检查代码与敏感数据的交互。该技术可识别出对关键数据构成真正威胁的漏洞，包括其他技术无法检测到的复杂漏洞和逻辑缺陷。

## 立即开始使用 Seeker

- **无缝融入 CI/CD 工作流程。**本机集成和 Web API 能够与您所使用的工具进行整合，无论是用于内部开发、基于云计算的开发、基于微服务的开发还是基于容器的开发。
- **快速轻松地部署。**Seeker 提供实时分析能力，误报率接近于零，而且能够开箱即用。
  - 完完全全的开箱即用，无需大量配置或调整
  - 无需网站登录证书或特殊扫描
  - 主动验证功能纳入了输入内容验证库和自定义功能，以便清理输入内容（例如，SQL 注入漏洞）
  - 可在大型企业环境中扩展
- **几乎适用于任何类型的测试方法。**Seeker 的非侵入式被动监控选项使其能够适用于现有的各种自动化测试、QA/dev 测试、自动网络爬虫、单元测试，等等。

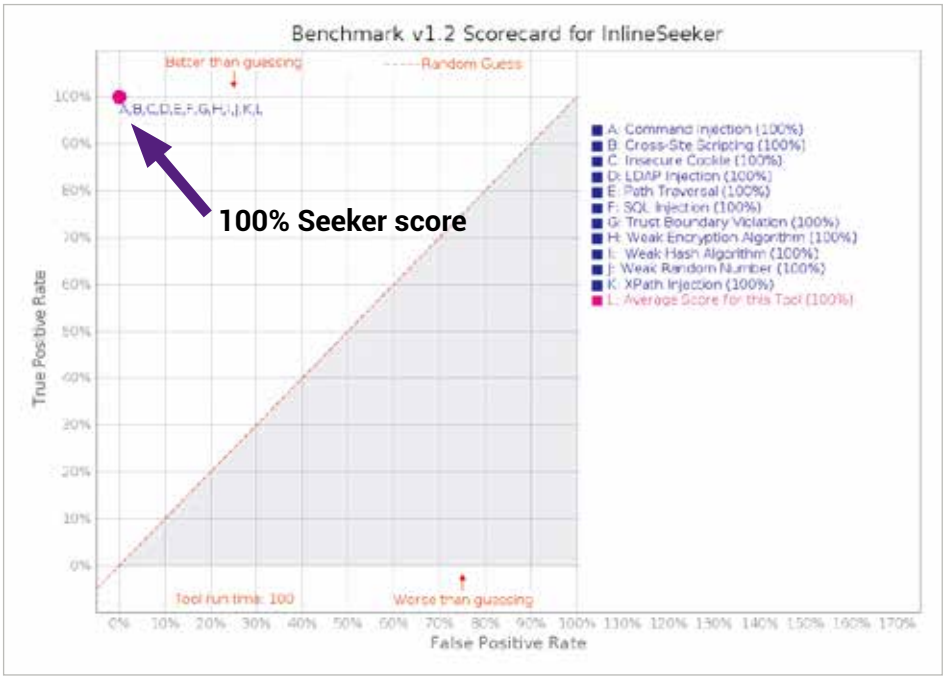
## URL 发现以及 Web 应用覆盖

自动 URL 映射提供了关于 Web 应用测试覆盖范围的清晰视图，并以图形化方式显示已经测试过的内容。您可以轻松地比较同一应用程序不同版本之间的覆盖范围差异。

## 敏感数据跟踪

Seeker 跟踪敏感数据的独特能力为业界首创。用户可以将数据标记为敏感数据（例如，信用卡号码、用户名以及密码），只要这些数据以未机密的方式存储在日志、数据库或文件中这些数据随时能够得到跟踪。跟踪敏感数据可帮助您实现对 PCI DSS 中要求数据加密章节的合规性，也能够帮助您遵守诸如 GDPR 等其他行业标准和法规。与人工检查相比较，这能够显著提高生产率并节省时间，同时也能够节省成本和资源。

## 最高的 OWASP 基准测试得分



SYNOPSYS®

# Seeker
# Technical Specifications

## 支持的语言

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

## Supported platforms

Languages/testing platforms

- Java
  - Any Java EE server
  - 任何 Java EE 服务器
  - GlassFish
  - JBoss
  - Tomcat
  - WebLogic
  - WebSphere
- .NET (2.0 或更高版本 )
  - IIS
- Node.js (6 或更高版本 )
  - Express
  - Hapi
  - Koa

## 运行时 / 框架

- .NET/CLR
  - ASP.NET MVC
  - 企业库
  - 实体框架
  - 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

## 技术

- 数据库
  - DB2
  - HSQLDB
  - MongoDB
  - MS SQL
  - MySQL
  - Oracle
  - PostgreSQL
- 应用类型
  - Ajax
  - JSON
  - Microservices
  - Mobile (over HTTP/S)
  - RESTful
  - 单页应用
  - SOAP
  - Web ( 包括 HTML5)
  - Web APIs
  - Web 服务

## Synopsys 公司的与众不同之处

Synopsys 公司帮助各种开发团队构建安全、高质量的软件，将风险降至最低水平，同时最大限度提高速度和生产力。Synopsys 公司是应用安全性领域的公认领导者，其提供的静态分析、软件组成分析以及动态分析解决方案能够让各个团队快速发现和修补私有代码、开源组件以及应用行为中的漏洞和缺陷。凭借其行业领先的工具、服务和专业知识的组合，只有 Synopsys 公司能够帮助企业在 DevSecOps 工作中以及在整个软件开发生命周期中最大限度地提高安全性和质量。

**有关详细信息，请访问** www.synopsys.com/software.

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

美国销售：800.873.8193
国际销售： +1 415.321.5237
电子邮件：sig-info@synopsys.com


07/23/18.DS_Seeker_0718