开源网安 SECZONE GROUP | VulHunter

VulHunter

产 品 手 册

开源网安灰盒安全测试平台

www.seczone.cn

公司概况

公司简介

SecZone 开源网安成立于 2013 年 5 月，是国内软件安全行业创领者和领先的软件安全开发生命周期

（S-SDLC）解决方案提供商，专注于软件安全领域的技术研究。SecZone 开源网安团队由来自思科、微软、惠普、Google、华为等行业顶级的安全专家组成，团队成员从业经验均为 10 年以上。SecZone 开源网安总部在深圳，同时在北京、广州、武汉、合肥、成都、南宁设有分支机构。

SecZone 开源网安始终以自主创新为发展源动力，以 S-SDLC 解决方案为核心，以 S-SDLC 平台为载体，向不同行业的客户提供覆盖软件开发全生命周期的软件安全开发咨询和落地服务，包括但不限于安全开发培训、安全需求识别、安全架构设计、安全代码实现、安全确认、安全审核及安全运营的完整业务生态，同时提供配套的工具链支持。帮助客户提升软件安全开发能力，构建安全可靠的软件产品。

未来，SecZone 开源网安将持续聚焦软件安全领域，努力成为全球软件安全领域极具竞争力的领导品牌。

公司愿景：让企业交付更安全的软件**核心价值**专业、开源、信赖

联系方式：电话：4000-983-183 网址：www.seczone.cn

邮箱：service@seczone.cn

微信公众号

版权声明

VulHunter 产品手册

开源网安灰盒安全测试平台（简称 VulHunter）是国内首款**自主研发**基于 IAST 技术的灰盒安全检测产品，拥有数十项发明专利，专注于 DevSecOps 中的应用安全领域，具有高覆盖、低误报、实时检测等优点，从容应对现有应用安全测试技术面临的诸多挑战。

本操作手册提供 VuHunter 平台以下信息：

- VuHunter 概述
- VuHunter 快速入门
- 产品功能说明

1 VuHunter 概述

下面几节重点介绍本文档编写的目的、平台介绍以及对平台使用角色的介绍和说明。

1.1 文档目的

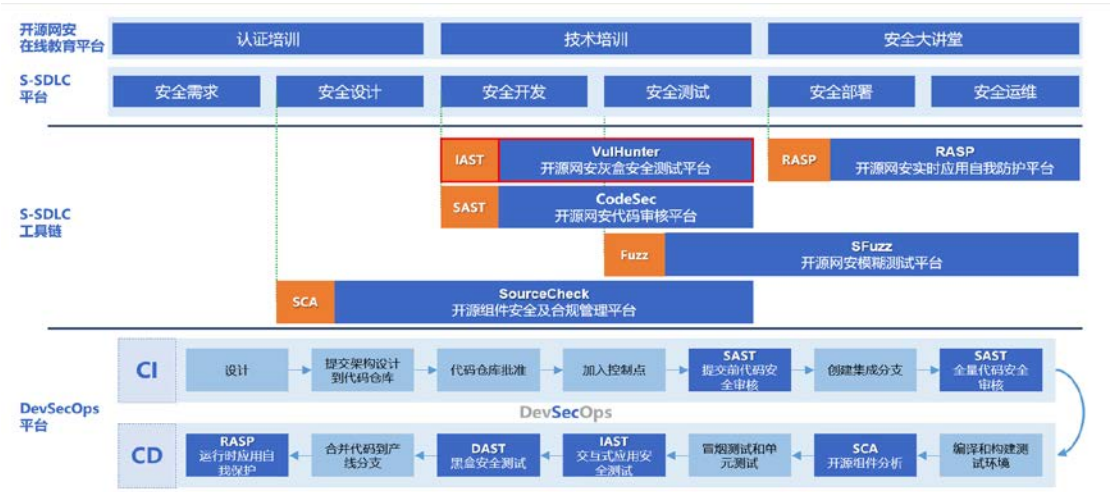
为了帮助开源网安灰盒安全测试平台（简称 VulHunter）的用户更好地了解和使用该平台,提高用户与平台的亲和度。该手册简述了平台的系统架构图、功能清单、软件性能、产品的主要参数以及系统的操作指导，以及该软件使用过程中应注意的一些问题。

1.2 平台介绍

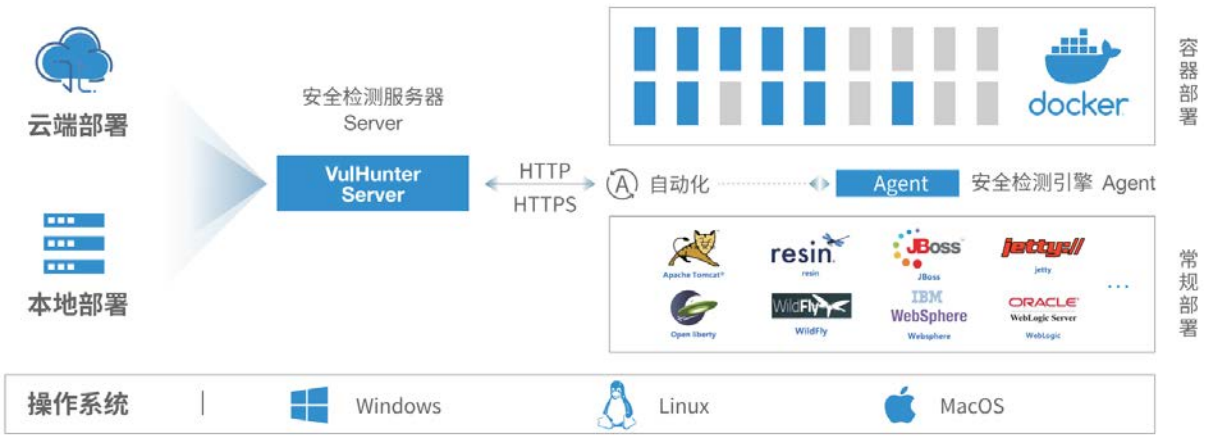
开源网安灰盒安全测试平台（简称 VulHunter）是国内首款**自主研发**基于 IAST 技术的灰盒安全检测产品，通过代理和在服务端部署的 Agent 程序，收集、监控 Web 应用程序运行时请求数据、函数执行，并

与扫描器端进行实时交互，高效、准确的识别安全漏洞，同时可准确确定漏洞所在的代码文件、行数、函数及参数。

VuHunter 覆盖 Java、PHP、Python、Node.js、.NET/C#/Framework、Go 等编程语言，支持多达 90+种安全漏洞的检测；扫描结果精准呈现，界面简明易于操作；提供多种集成方式，更加适用于 DevSecOps 等场景。



支持在云端及本地部署，Agent 可安装在各种适配的 Web 应用服务器中，或是在 docker 中安装，实现安全弱点的识别、归类、整理及上报等功能，通过 HTTP/HTTPS 方式上传至管理后台，实现整个测试。支持 Windows、Linux、MacOS 等操作系统部署及检测。



与基于 SAST 和 DAST 技术的产品相比，VulHunter 通过字节码插桩应用程序能获得更多准确的运行时信息。下表是 VulHunter 与 DAST 和 SAST 关于能获取到的信息类型对比。

获取信息类型	SAST	DAST	VulHunter
http 请求		√	√
http 响应		√	√
数据流	√（静态）		√
第三方软件			√
配置数据			√
后端连接信息			√

1.3 角色介绍

VuHuter 平台的用户主要包括：超级管理员、企业管理员、小组管理员、普通用户。企业管理员的账号由超级管理员添加，企业管理员添加小组管理员，小组管理员添加普通 用户。CodeSec 平台有一下四种用户角色：

· 超级管理员：企业组用户，由 VuHunter 技术支持人员直接创建，拥有者创建企业、企业管理员，设置企业级规则以及配置企业内操作列表权限。

· 企业管理员：企业级用户，由超级管理员登陆后创建。权限包括：查看所有小组检测到的安全弱点信息，跟踪漏洞，管理项目、查看企业数据看板、安全弱点报告、配置检测规则、权限设置等。

· 小组管理员：团队级用户，由企业管理员登录后创建。团队管理员的权限包括：给本团队添加普通用户，创建项目，扫描项目，查看项目中检测到的安全弱点信息，跟踪漏洞，查看小组数据看板，查看安全弱点报告、配置检测规则等。

· 普通用户：团队的普通成员，由小组管理员登录后添加。权限包括：创建项目、扫描项目，查看项目中检测到的安全弱点信息，跟踪漏洞，查看个人数据看板，配置检测规则等。

2 快速入门指南

VulHunter 是基于功能测试驱动的被动检测技术，即在开发工程师、测试工程师或者自动化测试脚本进行功能测试的同时，实时分析软件安全弱点。其使用和检测流程如下图。

图 VulHunter 使用和检测流程

检测流程说明：

1) 开发人员编写代码，完成后，提交到代码库；
2) 从代码库拉取代码，在编译环境中进行编译、发包；
3) 将编译好的应用包放置到 Web 应用服务器中，测试人员（研发、测试、安全等）将 agent 探针放置到同个 Web 应用服务器下，进行配置、启动，随应用启动后，可以根据功能测试用例进行功能测试；
4) 在进行功能测试的同时，agent 检测、发现安全弱点，实时上报到 VulHunter 管理平台；
5) 测试人员可登录 VulHunter 管理平台查看安全弱点信息，进行增、删、改、查等系列操作。

3 产品功能说明

常见安全弱点检测

VulHunter 已经支持近 90 种安全弱点的检测，能对应用程序执行覆盖了 OWASP Top 10、CWE/SANS Top 25 以及 PCI DSS 等所包含常见安全弱点的检测。

软件组件信息检测

VulHunter 支持对应用程序依赖的第三方软件信息的检测，为开发团队准确识别和记录所依赖第三方软件的完整信息，帮助开发团队有效管理第三方软件的使用。检测的第三方软件信息包括第三方软件的版本信息、发布时间、最新版本信息、最新版本的发布时间、当前版本包含的 CVE 公开漏洞信息等。

敏感信息跟踪

VulHunter 能自动识别身份证，银行卡号、用户标识、令牌等敏感信息，并跟踪其是否经过了不安全的传输或者处理，以及保护不足导致的信息泄露。使用者可以根据实际情况，定义自己的敏感数据类型。

提供完整的安全弱点信息

VulHunter 可提供完整的安全弱点检测信息，包括安全弱点的描述、风险、引入点、请求信息、数据流和修复方案等。

企业级的安全弱点管理

VulHunter 支持多级管理，每个企业管理员都可以创建若干个部门，且不同部门之间的数据都是互相独立的，对于不同角色的用户，都可展示对应的数据统计信息。

系统集成对接

VulHunter 检测出来的安全问题，可与企业已有的邮件系统、缺陷管理平台、工作跟踪平台集成对接。

捍卫中国软件安全