悬镜
XMIRROR

源鉴 SCA 开源威胁管控平台
操作手册

文档说明

文档名称	源鉴 SCA 开源威胁管控平台操作手册
文档版本	V3.9
保密级别	客户级
更新日期	2023 年 8 月 4 日

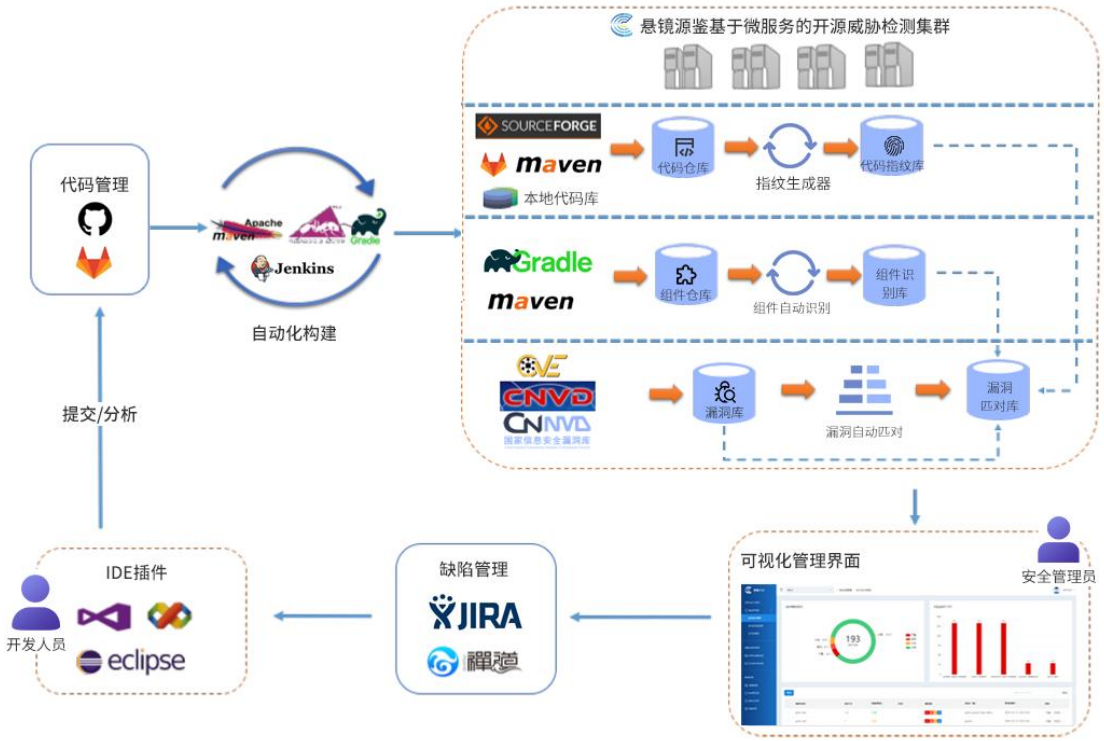
版权声明

目录

一. 平台介绍

1.1 平台介绍

悬镜源鉴开源威胁管控平台（以下简称“源鉴 SCA”）基于多源 SCA 开源应用安全缺陷检测技术，结合悬镜独有的应用探针技术，精准识别应用开发过程中软件开发人员引用的第三方开源组件，并通过应用组成分析引擎，多维度提取开源组件特征，计算组件指纹信息，深度挖掘组件中潜藏的各类安全漏洞及开源协议风险。相比于传统的 SCA 检测平台，源鉴 SCA 引擎更加侧重应用系统实际运行过程中动态加载的第三方组件及依赖，在此基础上进行深度且更加有效的威胁分析。同时，本平台通过智能化数据收集引擎在全球范围内获取开源组件信息及其相关漏洞信息，及时获取开源组件漏洞情报，降低由开源组件带来的安全风险，保障软件安全。



源鉴 SCA 原理

1.2 CNNVD 兼容性说明（引自《CNNVD 兼容性服务白皮书》）

（1）什么是 CNNVD?

国家信息安全漏洞库（“China National Vulnerability Database of Information Security”，简称“CNNVD”），是中国信息安全测评中心为切实履行漏洞分析和风险评估的职能，负责建设运维的国家信息安全漏洞库，为我国信息安全保障提供基础服务。通过自主挖掘、社会提交、协作共享、网络搜集以及技术检测等方式，经过多年的收录工作，CNNVD 已收录信息技术产品漏洞信息 8 万余条，信息系统相关漏洞信息 6 万余条，漏洞信息覆盖国内外主流的应用软件、操作系统和网络设备等，涉及国内外各大厂商上千家，涵盖政府、金融、交通、工控、卫生医 疗等多个行业。随着 CNNVD 漏洞库漏洞数量不断扩大、影响力逐步提升，目前成为收录漏洞数目最多、漏洞属性最全、内容质量最高的国家级信息安全漏洞库。

CNNVD 作为国家信息安全漏洞库，通过多年建设经验积累，对国内信息安全技术国家标准，及国际通用标准进行了分析与研究，并以国家标准为基础，参考国际通用标准，完成了国内外主流漏洞库的漏洞信息资源规范化的整合，建立了规范统一漏洞数据标准，包括：《CNNVD 漏洞编码规范》、《CNNVD 漏洞命名规范》、《CNNVD 漏洞分级规范》、《CNNVD 漏洞内容描述规范》、《CNNVD 漏洞分类描述规范》、《CNNVD 漏洞影响实体描述规范》。

CNNVD 漏洞库对所收录的漏洞信息给予统一的编码标识（即：CNNVD-ID 标识），建立了与国内外主流漏洞库的映射关系，同时对漏洞详细属性特征进行统一的、详细的、标准化的描述（如：漏洞命名、内容描述、分类、分级等），基本涵盖了国内外主流软硬件产品和信息系统。

以丰富标准的漏洞数据为依托，规范详实的漏洞描述为基础，国家信息安全漏洞库（CNNVD）对国内外信息安全厂商及用户推出兼容性服务，为漏洞挖掘、

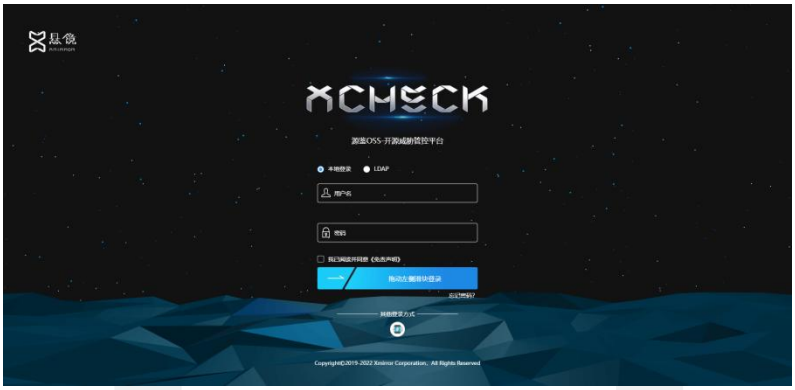
应用、验证与规避等技术研究提供基础支持，为开发更安全的信息产品或软件系统提供理论和技术支撑，进一步满足国家重要信息系统安全保障的需求。

（2）本产品兼容 CNNVD 漏洞库

CNNVD 兼容性是指通过使用 CNNVD 标识，在各类安全工具、漏洞数据存储库及信息安全服务之间，以及与其他漏洞披露平台之间，实现漏洞信息交叉关联的方式。CNNVD 兼容性服务是 CNNVD 面向国内外信息安全从业单位，对其产品/服务等涉及的漏洞信息进行规范性评估与认证的服务。通过 CNNVD 兼容性服务的信息安全产品/服务，可实现其漏洞信息拥有统一的规范性命名与标准化描述，从而提高和加强国内信息安全行业漏洞信息资源的共享与服务能力。本产品兼容 CNNVD 漏洞库，漏洞库更新频率与 CNNVD 漏洞库基本保持一致。

二. 登录

2.1 登录

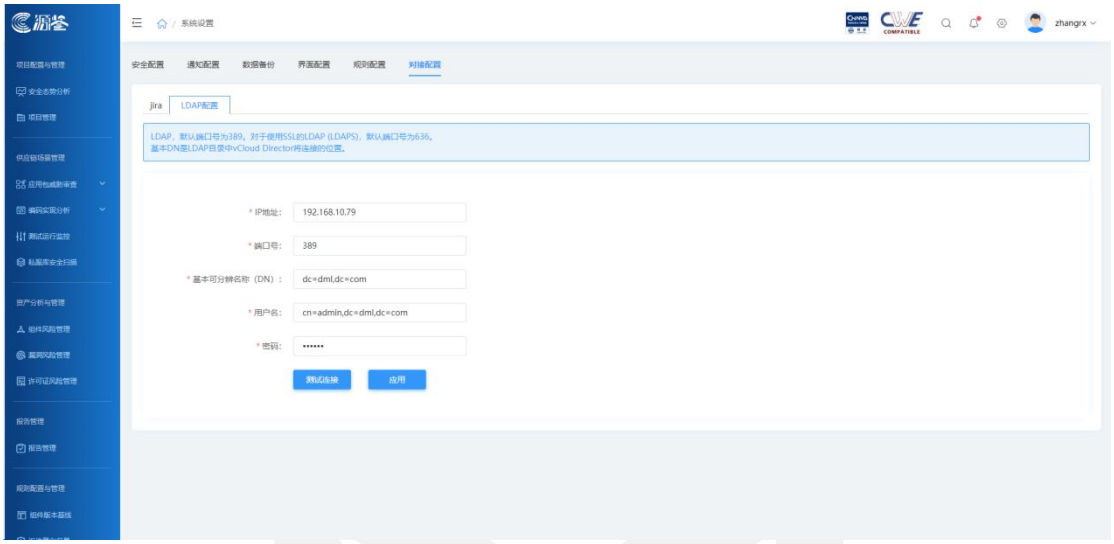


2.1.1 本地登录

输入用户名及密码，阅读免责声明，并进行人工验证。验证成功后进入平台。首次登录时，采用默认的超级管理员账号密码（请联系技术人员获取）登录即可。

2.1.2 LDAP 登录

在使用 LDAP 登录功能之前，需要进行 LDAP 对接配置。点击进入【系统设置】-> 【对接配置】 -> 【LDAP 配置】：



配置说明：

参数名称	默认值	是否必填	参数描述
IP 地址	无	是	部署 LDAP 服务的 IP
端口号	389	是	部署 LDAP 服务开放的端口号
基本可分辨名称（DN）	无	是	基本 DN 是 LDAP 目录中 vCloud Director 将连接的位置
用户名	无	是	LDAP 的用户名
密码	无	是	LDAP 的密码