羚见数据安全检查工具箱 SEC6000-RAS-DCBox

用户手册

版本： V6.0.3.1（20240703）

密级： 受限公开

■ 版权声明

■ 内容声明

您购买的产品、服务或特性等受合同和条款的约束，本文档中描述的部分功能可能不在您的购买或使用范围之内。

本文档仅作为使用指导，实际产品可能会由于版本升级或其他原因，与文档描述有略微差异。

■ 免责声明

在使用产品之前，请详细阅读免责声明，一旦开始使用，即认可和接受本声明的全部内容。在使用过程中，领信数科不对以下情况承担任何责任：

•因系统运维或管理人员未及时处理影响系统稳定性和可用性的告警，而造成的数据损失、系统可用性降低等情况。

•因业务量超过所规划硬件能力而造成的数据损失、系统可用性降低等情况。

•因自然灾害（包含但不限于水灾、火灾、地震等）或外部原因（包含但不限于断网、断电等）而造成的数据损失、系统可用性降低或不可用等情况。

■ 格式约定

•**粗体字**：菜单、命令和关键字

•*斜体字*：文档名、变量

•**说明**：对描述内容的补充和引用信息

•**提示**：使用设备时的技巧和建议

•**注意**：需要特别注意的事项和重要信息

•**警告**：有可能造成人身伤害的警告信息

目 录

前　言

内容简介

章节	概述
1.产品概述	介绍 DCBox 的背景、体系结构、部署方式、产品定位等信息。
2.登录	介绍 DCBox 的登录的功能。
3.典型策略配置案例	介绍 DCBox 的典型策略配置案例。
4.资产管理	介绍 DCBox 的资产扫描、资产预览等的相关功能。
5.脆弱性检测	介绍 DCBox 的系统扫描、WEB 扫描、弱口令扫描等的相关功能。
6.脆弱性模板	介绍 DCBox 的基线策略模板等的相关功能。
7.流量探测	介绍 DCBox 的流量探测等的相关功能。
8.敏感探测	介绍 DCBox 的敏感探测等的相关功能。
9.合规检查	介绍 DCBox 的法规合规检查、知识库等的相关功能。
10.报告中心	介绍 DCBox 的资产报告导出、脆弱性导出等的相关功能。
11.脆弱性模板	介绍 DCBox 的基线策略模板等的相关功能。
12.系统配置	介绍 DCBox 的资系统监控等的相关功能。

获得帮助

文档意见反馈

可以通过以下方式反馈在文档使用过程中遇到的任何问题和对文档的建议和意见。

邮箱：service@seclead.cn

售后服务

提供全国范围内的服务热线，可以帮助用户解决在使用安全设备和服务过程中遇到的各种问题和困难。

服务热线

网站：https://www.seclead.cn

服务电话：400-9919-700

一. 产品概述

本章主要内容如下：

功能	描述
背景	简单介绍 DCBox 产品的背景。
体系结构	介绍 DCBox 的体系结构。
部署方式	介绍 DCBox 的部署方式。
产品定位	介绍 DCBox 的主要功能。

1.1 背景

当今数字化时代，随着各种网络应用的广泛应用和互联网技术的不断发展，网络空间已成为人们生活和工作的重要组成部分。与此同时，网络安全问题也日益突出，网络攻击、数据泄露等事件频频发生，并且近年来，漏洞数量也呈快速增长的趋势，长期处于严峻状态，给企业安全带来了巨大的挑战，另外，除了脆弱性漏洞之外，各种流量中的隐含风险也时时刻刻影响着企业单位的安全，如各种是恶意攻击风险，比如黑客可能通过篡改或模拟请求、进行 DDoS 攻击等方式，使得 API 服务出现故障、崩溃甚至被控制，从而对系统造成巨大损失。

随着《网络安全法》、《数据安全法》、《个人信息保护法》等法律文件的相继颁布，各行业主管部门和地方政府也纷纷出台数据安全条例规范，国家开始进入数据安全强监管时代。如何准确、快速地评估自身数据资产的安全状态，如何针对资产中的各种难以洞察的脆弱性漏洞以及流量中的隐匿风险进行底数清，伴随着业务需求的产生，相应的解决方案也应运而生。

市面上针对资产脆弱性及流量探测领域均有较为成熟的产品来覆盖需求，但总体而言，能力集成较为分散，需要多种产品的组合，才能提供企业常规化的漏洞扫清与资产排查，为企业提供更有效，更便捷的自查自检方法，亟需一款综合性便携式设备。

1.2 体系结构

羚见数据安全检查工具箱（DC-Box）系统是架构于自有的网络操作系统之上，使用基于脚本插件的规则库来对目标系统进行黑盒测试的工具。具体架构如下图 1.2。

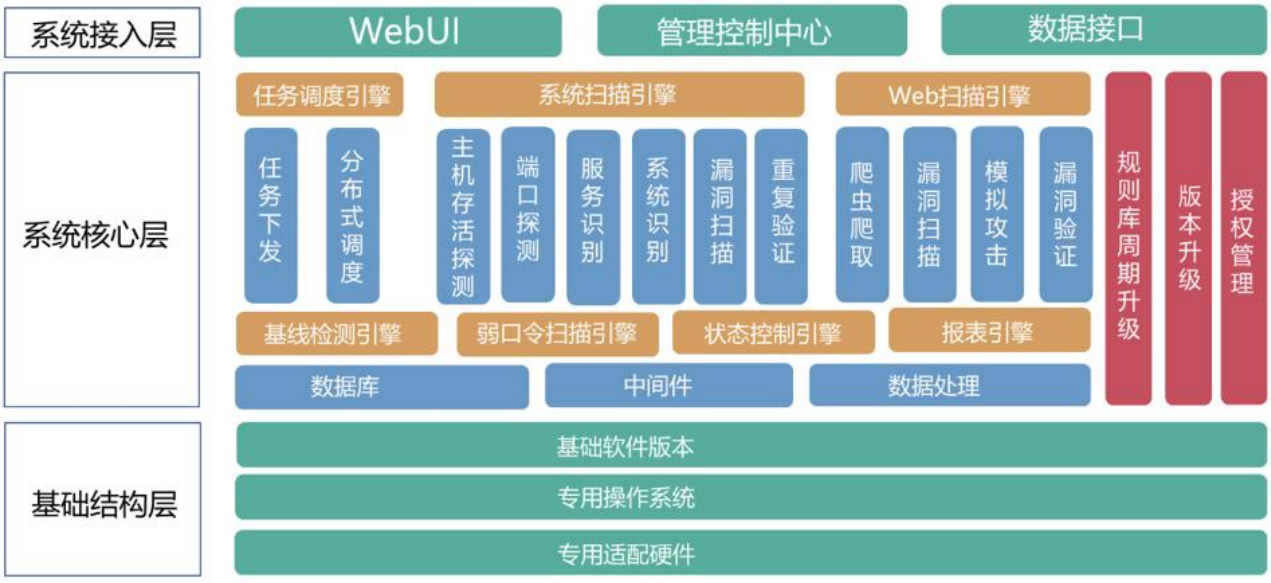


图 1.2 数据安全检查箱体系结构

➢任务调度中心

基于负载均衡、指定引擎等多种方式的任务调度模式。

➢插件引擎

高效的插件执行引擎，根据前置条件判断插件是否需要执行，减少多余的测试用例，同时根据端口、服务、版本、认证状况等多种情形提供脚本，检测出尽量多的安全问题，减少漏报。

➢爬虫引擎

用于对 Web 系统的页面获取，支持对 JavaScript、BOM（浏览器对象）、Flash 的解析。

➢端口、服务识别

漏洞扫描的基础模块，采用多种技术手段对端口进行探测，对于服务的识别不仅仅基于端口号，而是发送数据包来对服务器返回数据进行甄别从而判断服务的类型，大大提高了扫描结果的准确性。

1.3 部署方式

考虑到护网需求的常规化，DC-BOX 采用一体机式形态，即插即用，完全支持旁路部署在核心交换机上，对各个区域的设备进行扫描，单机部署操作简单，且不改变客户现有网络结构。具体拓扑结构如图 1.3 所示。

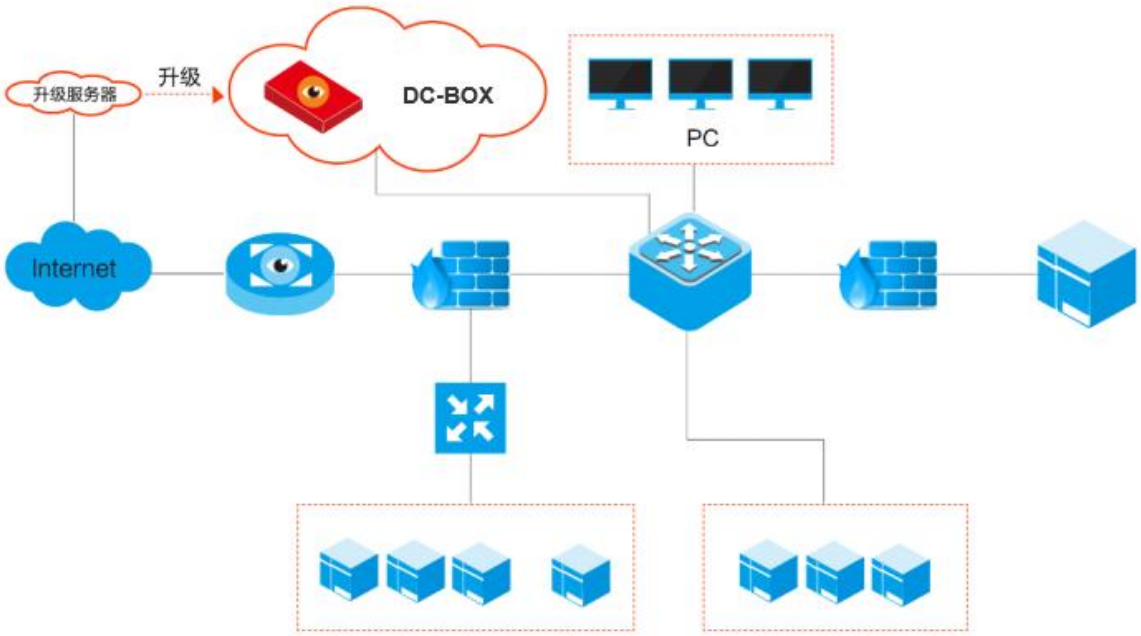


图 1.3 部署方式

1.4 产品定位

1.4.1 资产管理

资产扫描功能为 DC-BOX 的核心能力之一，通过主动扫描的方式，全方位洞悉系统内的核心资产，其中包括边界资产、web 资产、数据库资产、视频资产以及文件服务资产，并支持手动注册添加至资产台账，联动地域等信息，一体化测绘出不同区域的资产全景，给管理者提供有力的辅助决策支撑，实现资产全感知。当前资产管理模块主要有以下基本功能：

资产扫描：可实现对网络中的各类设备的扫描发现，可查看当前发现设备列表和历史发现情况，支持主动扫描探测等多种方式实现资产设备的发现。

区域配置与资产测绘：通过配置不同区域（省级，市级，区/县级，单位），形成区域字典，自动联动已注册资产，自动化测绘出不同区域资产分布情况，并全方位展示于资产测绘；

资产台账：实现对各类资产设备设备的信息维护、资产查询、和注册管理。可管理的资产包括边界资产、web 资产、数据库资产、视频资产以及文件服务资产等。

资产指纹识别：支持对设备类型的分析识别，通过检测设备操作系统、端口状态、设备厂商等多种信息，可准确分析出设备类型。系统预置交换机设备、服务器设备、网络安全设备、数据库服务器设备、边界交换设备等多种特征模型，支持设备类型分析模型的自定义配

量，可按照设备属性和运行参数等多种信息配量特征模型，包括设备端口、操作系统版本、设备厂商等内容。

1.4.2 脆弱性检测

系统漏洞扫描：主机系统上存储、处理和传输各种重要数据，一旦遭受攻击，将

可能导致程序运行失败、系统宕机、重新启动等后果，或者是获得主机上存储的敏感信息。更为严重的是，可以利用漏洞来执行非授权指令，甚至可以取得系统特权，从而控制整个主机，进而进行各种非法操作。

DC-BOX 支持针对网络环境中的各种主机、交换机路由器、防火墙、中间件等存在的常见漏洞、典型漏洞（如心脏出血）、0day 漏洞等进行扫描和检查。具体功能如下：

（1）支持扫描通用操作系统，涵盖 Windows 系列、苹果操作系统、Linux、AIX、HPUX、IRIX、BSD、Solaris 等。

（2）支持扫描交换路由设备，涵盖 Cisco、Juniper、华为、F5、Checkpoint、锐捷在内的主流厂商的设备。

（3）支持扫描安全设备，涵盖 Checkpoint、赛门铁克、Cisco、Juniper、Palo Alto、华为在内的主流厂商的防火墙等安全设备。

（4）支持扫描物联网设备，如主流厂商海康威视、宇视、华为、大华、Brickcom、索尼、TP-LINK、AXIS、佳能等的摄像头，三星、惠普、爱普生、佳能等厂商的打印机。

（5）支持针对工控专用设备包括 PLC、SCADA、DCS、工控专用网络设备的漏洞扫描。

（6）支持国产操作系统、数据库的扫描，国产操作系统包含中标麒麟、凝思、华为欧拉、深度、红旗、中兴新支点，国产数据库包括神通、人大金仓、南大通用、达梦。

（7）支持大数据组件框架漏洞检测，如 zookeeper、ElasticSearch、ActiveMQ 、Kibana、Hadoop 等。

Web 漏洞扫描：DC-BOX 提供广度和深度两种扫描方式，支持提供 OWASP 定义的 TOP 10 Web 威胁如注入（SQL 注入、Cookie 注入、Xpath 注入、代码注入、框架注入、Base64 注入、命令注入、操作系统命令注入）、XSS 跨站脚本、伪造跨站点请求（CSRF）、网页挂马、暗链、敏感信息泄露、安全配置错误等漏洞风险等漏洞扫描服务。通过基于爬虫的网站漏洞扫描技术，能够有效识别 Web2.0 以及 Flash，保障 Web 漏洞扫描的全面性。进行网站结构分析、漏洞分析，及时获得网站的漏洞情况，以及修补建议。

数据库漏洞扫描：采用先进的数据库发现技术和实例发现技术等，可针对当下主流的数据库，如 Oralce、MySQL、Postgres、IBMDB2、MongoDB、SQLServer、Informix、Sybase 等进行漏洞检测，包括对数据库系统的各项设置、数据库系统软件本身已知漏洞、数据库系统完整性进行检查和对数据库系统的整体安全性做出评估，并给出提高数据库安全性的修复建议。通过登录扫描可对数据库的系统表甚至字段进行安全检测。

安全基线检测：安全配置核查是安全管理的基本工作，同时也是安全运维的重要技术手段。安全配置核查首先要建立满足组织信息安全管理体系的安全配置要求的基线。当前，部分重要行业和监管部门已经针对行业的信息系统建立详细的安全配置要求及规范。它构建针对不同系统的详细检查项清单和操作指导，为安全运维人员的安全技术操作提供标准化框架和指导，有很广泛的应用范围，主要包括新系统的上线安全检查、第三方入网安全检查、安全合规检查、日常安全检查等。

DC-BOX 参考国内外标准、行业技术规范和安全运维最佳实践构建了以业务系统为核心，覆盖业务层、系统支撑层的安全配置基线模型。从业务系统安全要求出发，将要求分解到对应的支撑系统的具体安全要求。支撑系统包括操作系统、数据库、中间件和应用系统，还包括网络设备和安全设备等。针对这些支撑系统的具体产品类型如 Windows, Oracle, Weblogic, 交换机,防火墙等，根据具体的安全要求可细化到可执行和实现的具体要求，并可以对同类设备，不同品牌型号，形成具体的安全要求及配置检查方法。

弱口令扫描：对系统存在的弱口令做检测，支持知名的协议、数据库、中间件、

HTTP 服务、HTTPS 服务和摄像头检测如 TELNET、FTP、SSH、POP3、RDP、SMTP、Oracle、MySQL、PostgreSQL、MsSQL、Sybase、Informix、HTTP、大华摄像头、华为摄像头等。系统内置默认的字典库，并支持上传自定义的字典库，丰富平台弱密码检测能力。

1.4.3 流量探测

流量探测模块旨在于利用先进的技术和算法，实时捕获和解析网络中的 API 流量。通过深入分析和监控 API 请求和响应，帮助用户全面了解其流量片段内的 API 使用情况以及对应安全行为分析，以下是该功能的主要特点和优势：

实时监测和分析：无论是内部系统之间还是与外部第三方服务的交互。可以实时查看 API 请求和响应的详细信息，包括参数、状态码、返回结果等，便于快速定位和解决潜在的问题。

安全性评估：通过对 API 流量的深入分析，该产品能够评估 API 的安全性，并发现潜在的风险和漏洞。它可以识别出现的异常行为，并进行展示，将恶意行为以及潜在的安全威胁实现底数清，帮助用户及时采取预防和修复措施，保护 API 和敏感数据的安全。

报告导出与共享：用户可以根据需要将 API 流量监测和分析的结果导出为报告，方便内部团队评估和决策。此外，用户还可以选择共享报告给相关的合作伙伴和第三方，以加强沟通和合作，并共同提升 API 的质量和安全性。

总之，API 流量探测功能能够为用户提供全面的 API 监测、安全性评估和不安全内容溯源，并提供相关详细报告的导出，这将帮助用户及时发现和解决流量中的相关隐匿风险，确保了系统的稳定性、安全性、保密性和完整性。

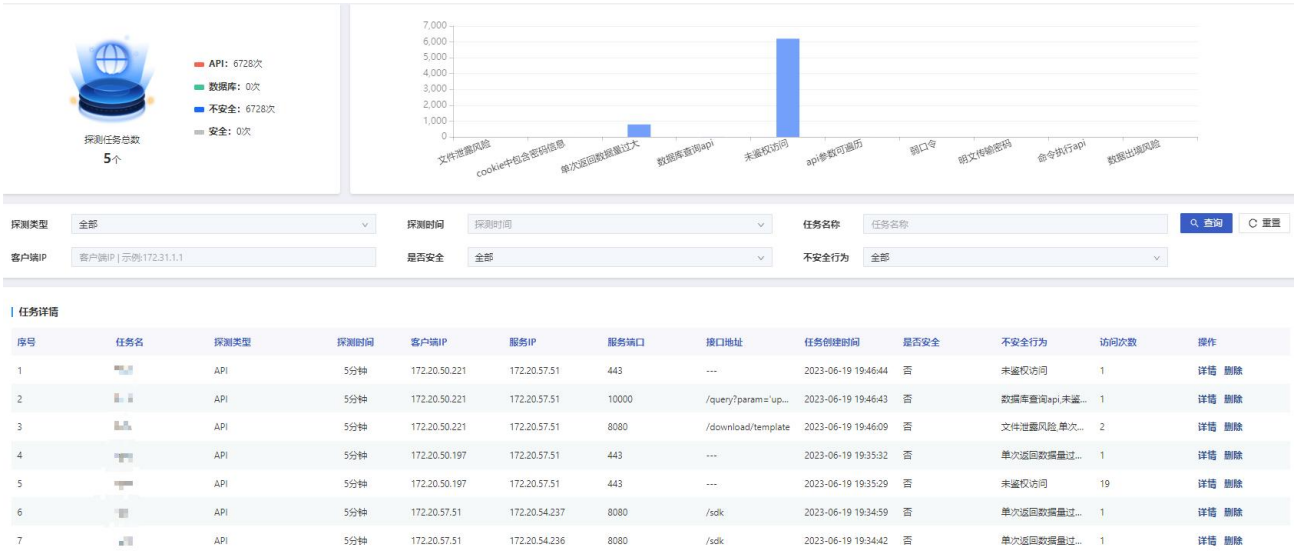


图 1.4.3 流量探测

1.4.4 报告中心

DC-BOX 支持资产台账、脆弱性全览以及流量探测预览的多种报告生成，并支持自选维度，自定义的报告生成，包括报告名称、报告组件、可视化模块、及文字编辑等多样式，且支持报告的预览与导出。

资产台账报告：统计资产数量，设备分类，资产类型等全方位的资产信息并整理汇总，支持自定义分析与编辑；

脆弱性漏洞报告：统计漏洞数量、整改数量和整改率等各项数据，对数据进行报表化，定期完成对所管辖资产的漏洞关联，形成漏洞统计报告；

流量探测预览报告：统计 API 流量探测的所有安全行为与不安全行为，并根据 API 模型分类展示不安全行为的详细内容，便于分析与溯源。

二. 登录

笔记本电脑配置 192.168.0.X/24 的 IP 地址，并直连到 DCBOX 设备管理接口，默认为 MGT 或 ETH0 接口。打开浏览器(推荐谷歌或火狐浏览器)，输入 https://192.168.0.52 访问数据安全检查工具箱. 登录首页面

图 2 登录

三. 资产管理

3.1 资产扫描

3.1.1 扫描任务

3.1.1.1 扫描任务--任务列表

任务列表分为待扫描、扫描中、已完成页面。

待扫描页面可进行新建任务、编辑、删除、开始扫描、批量删除等操作。

图 3.1.1.1-1 待扫描页面

WEBUI：主界面 -> 资产扫描 -> 扫描任务 -> 新建任务

新建任务页面可进行扫描方式、资产类型的选择，还可进行白名单的设置。

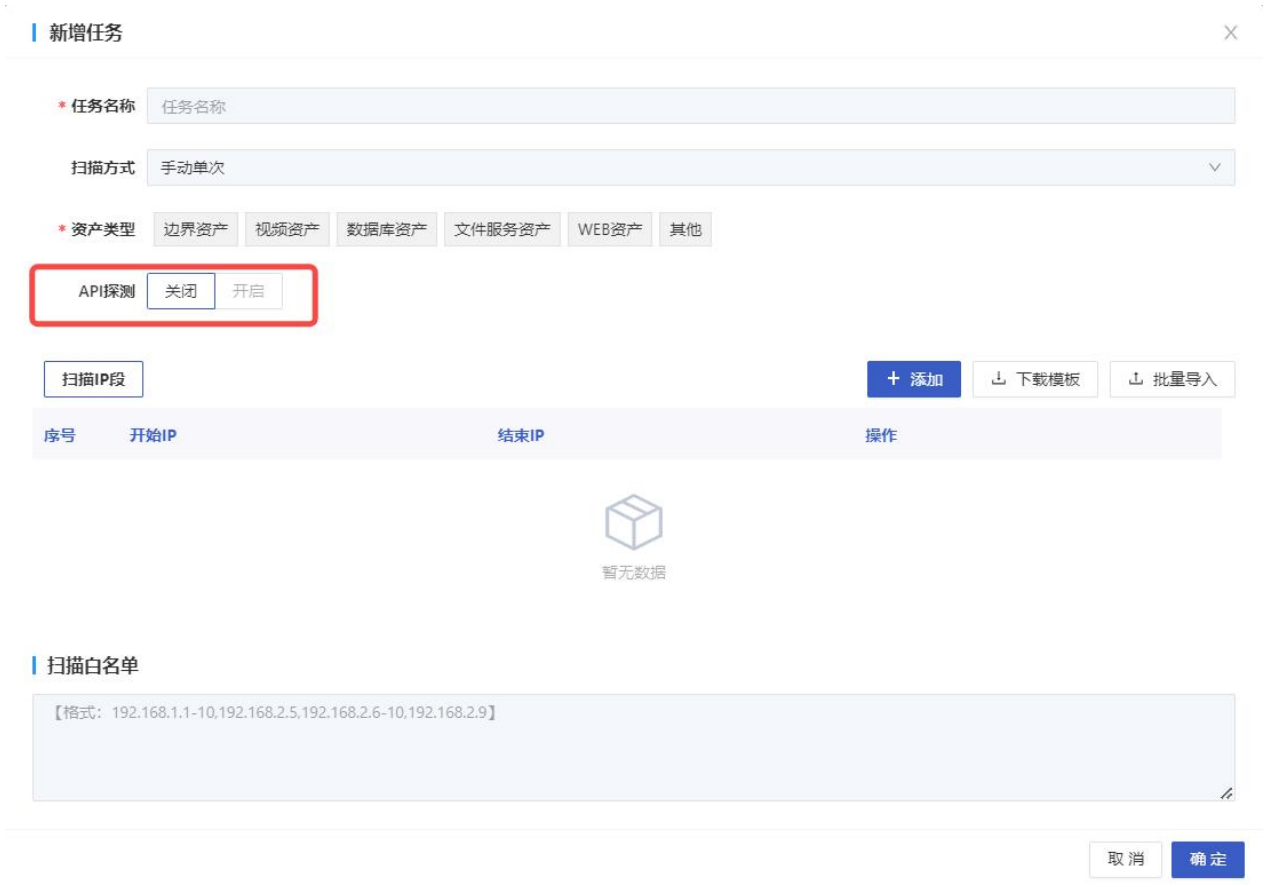


图 3.1.1.1-2 新建任务

新建任务参数说明如表 3.1.1.1-1 所示：

表 3.1.1.1-1 参数说明

参数	说明
任务名称	资产扫描任务的名称
扫描方式	资产扫描定时方式；分别为手动单次、即时单次、每 30 分钟、每小时、每天、每周、每月、每 3 个月、每 6 个月、每年
资产类型	扫描的资产类型：可选项分别为边界资产、视频资产、数据库资产、文件服务资产、WEB 资产
API 探测	API 探测关闭，不进行 api 资产的扫描，API 探测开启，进行 api 资产的扫描，包括 http 与 https 的资产
任务列表	可填入开始 IP：192.168.0.1　　结束 IP：192.168.0.255
扫描白名单	可填入 IP/IP 范围，扫描时跳过该 IP/IP 范围的资产，不进行该资产的扫描

扫描中的页面可停止扫描。

图 3.1.1.1-3 扫描中页面

已完成页面可进行新建任务、批量删除、删除、重扫、查看、下载等操作。

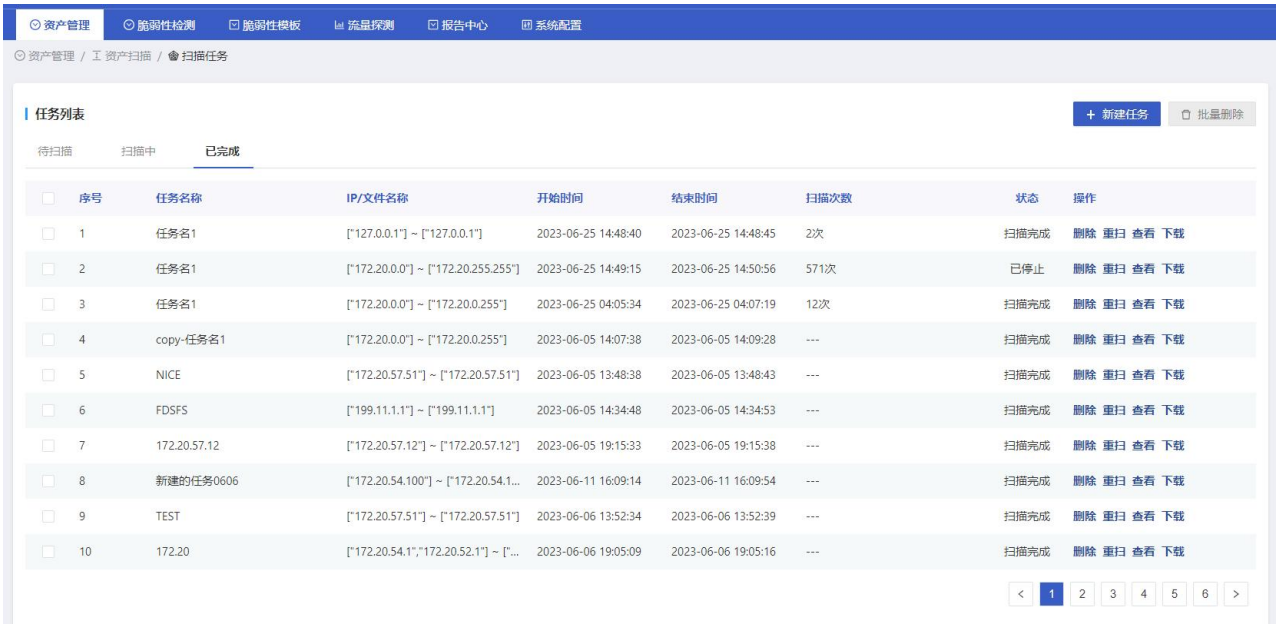


图 3.1.1.1-4 已完成页面

3.1.1.2 扫描任务--新识别资产

新识别资产展示扫描任务中新发现的资产列表，可进行添加、删除、批量添加、批量删除等操作。添加后的资产在资产预览-资产台账处展示，资产来源为扫描。

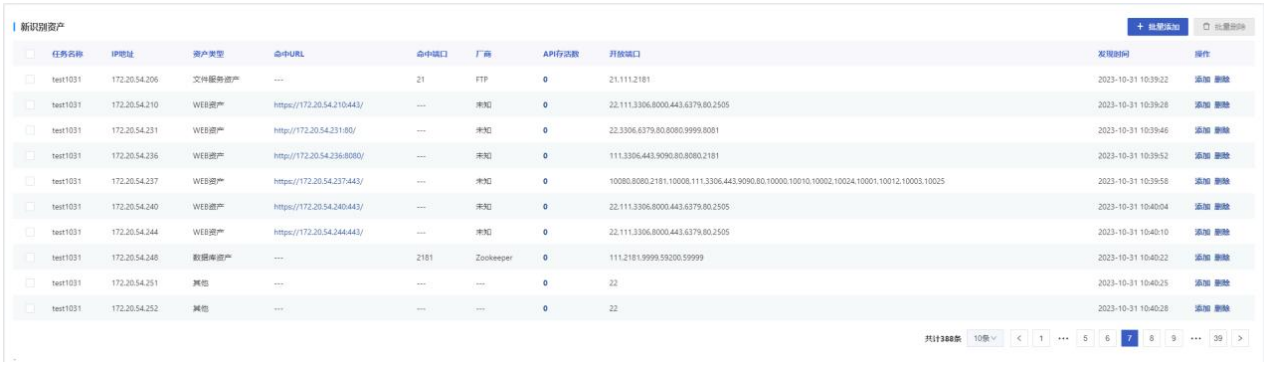


图 3.1.1.2-1 新识别资产列表

3.1.2 扫描结果

扫描结果展示已扫描出的资产，扫描结果列表展示注册过及未注册的资产，可进行添加、删除、批量添加、批量删除、导出发现列表等操作；支持资产类型、厂商名称、IP 地址、设备分类、是否注册、区域名称的查询。

扫描结果分为常规列表、探索列表，对边界、web、数据库资产指纹进行分类与二次验证，提升资产扫描精准度。

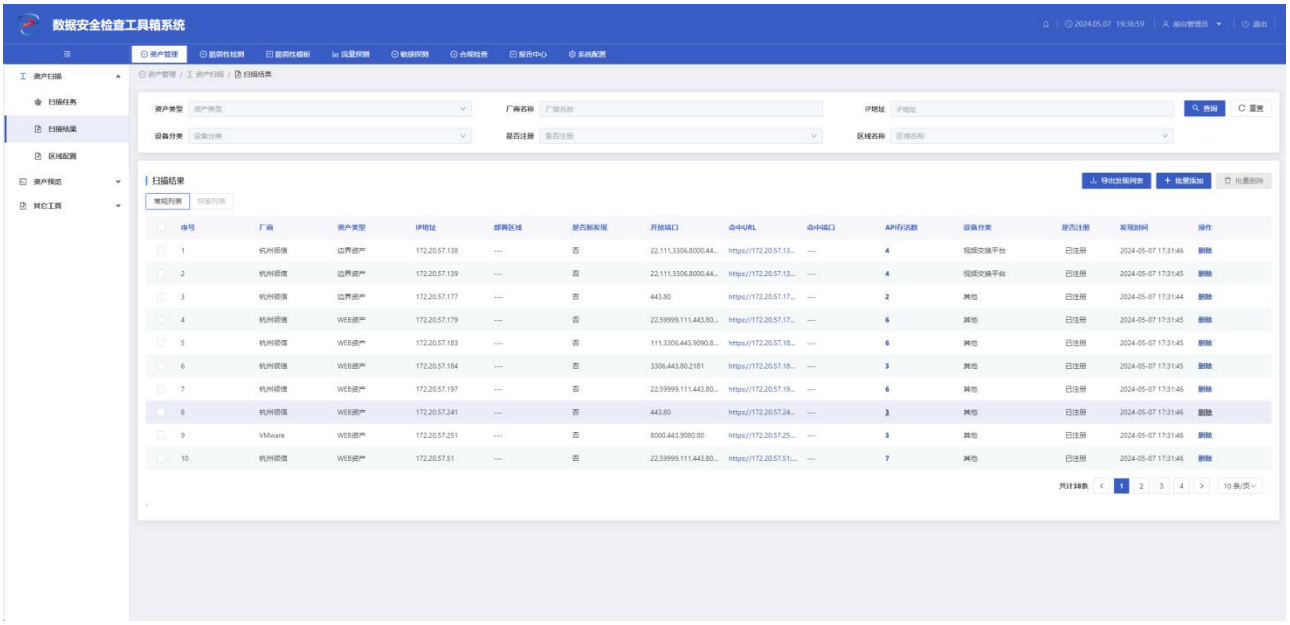


图 3.1.2 扫描结果

3.1.3 区域配置

区域配置把对应资产与相关区域对应起来，方便“资产测绘”页面的展示，点击“新增”按钮，弹出新增配置的页面，配置区域为必填项。

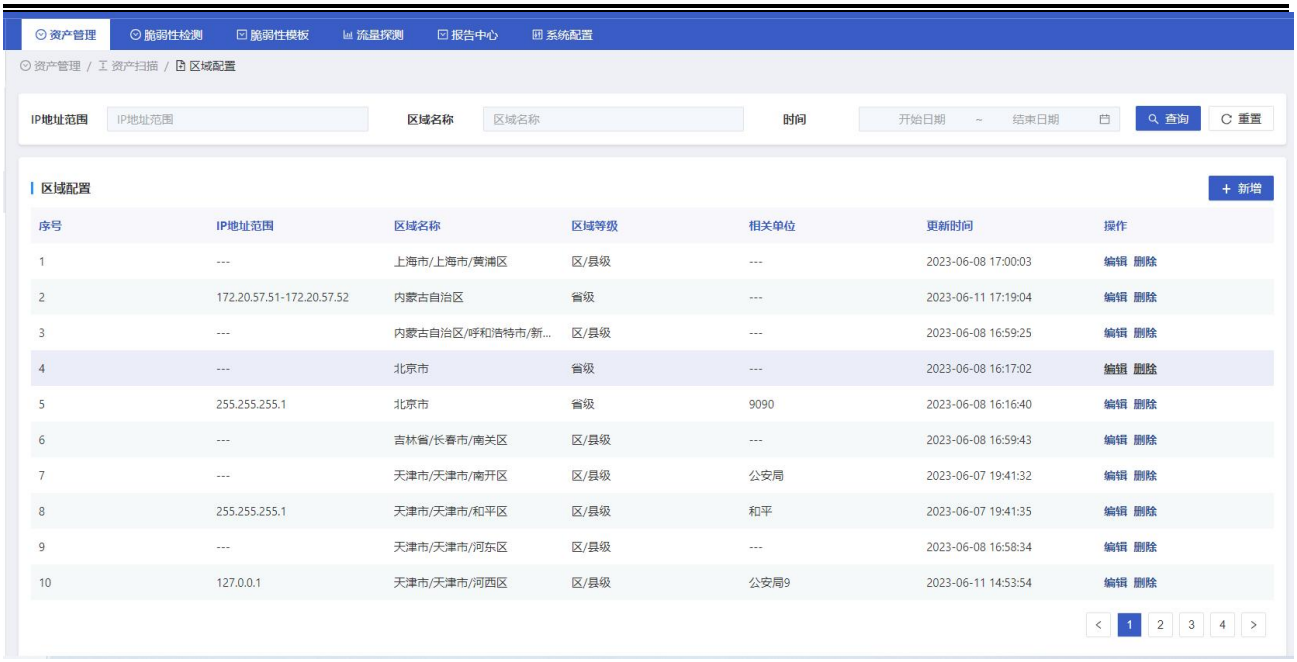


图 3.1.3 区域配置

3.2 资产预览

3.2.1 资产台账

资产台账展示已注册的资产列表，分级展示区域配置中新增的配置级别。支持区域、资产名称、资产类型、设备分类、资产 IP 地址查询。支持列表导出操作。

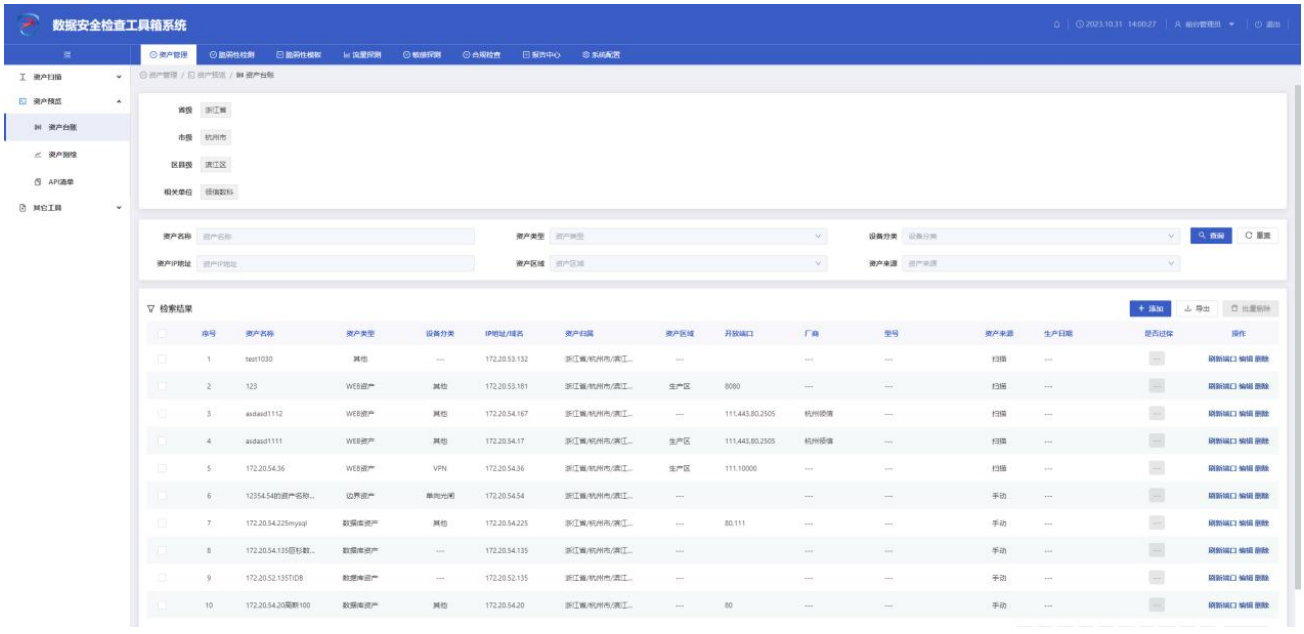


图 3.2.1 资产台账

点击“新增”，展示新增资产相关弹窗，有 17 个输入项，其中资产名称、资产类型、资产归属、资产 IP 为必填项。

图 3.2.2.1 新增资产

3.2.2 资产测绘

资产测绘可视化展示所有已注册资产的区域归属情况及不同区域资产的分布情况。左上可进行区域筛选，每个区域右上角均有+按钮，点击将从下方出现相关区域的资产概况，右侧可进行资产展示的放大、缩小、自适应、全屏、退出全屏、切换布局、全选节点、取消全选操作。

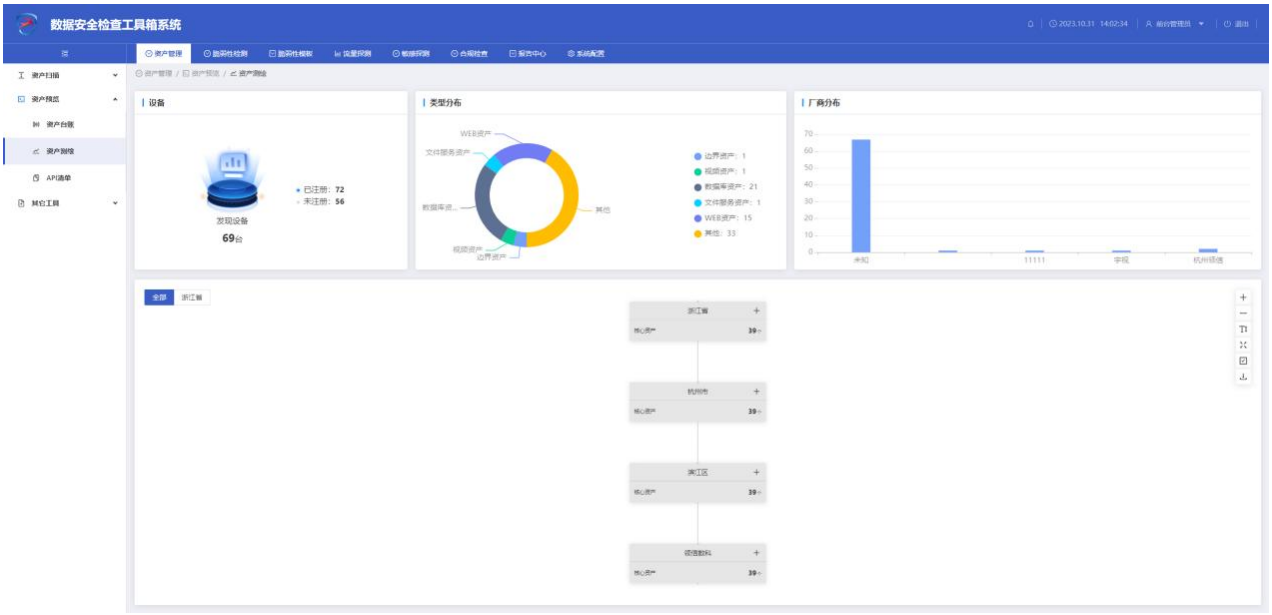


图 3.2.2 资产测绘

3.2.3 API 清单

API 清单展示资产扫描与流量探测处扫描出的 API 资产列表，可进行资产名称、资产分类、API 来源的筛选操作。

点击“添加”，可手动添加 API 清单列表。

图 3.2.3-1 添加 API

API 清单展示手动添加、资产扫描、流量探测来源的数据。

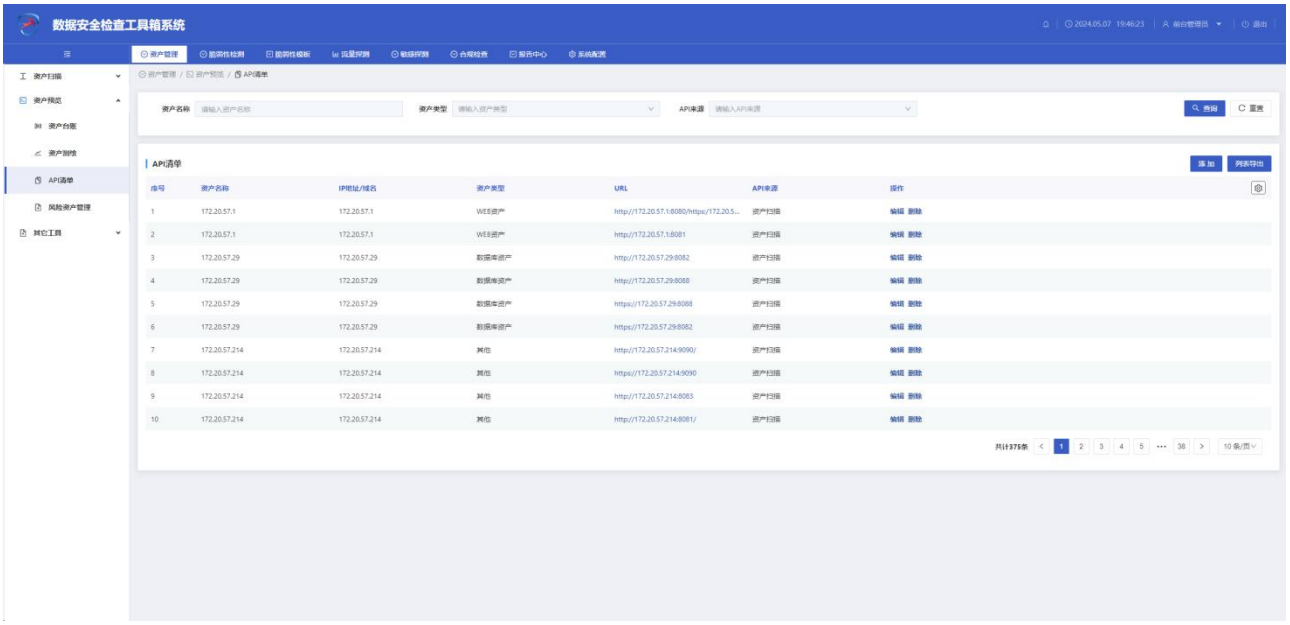


图 3.2.3-2 API 清单

点击“列表导出”，导出当前列表的 API 清单数据。

3.3 其他工具

3.3.1 设备端口扫描

设备端口扫描可通过 ip 地址检索并查看相关的设备启用的端口，支持设备端口导出。

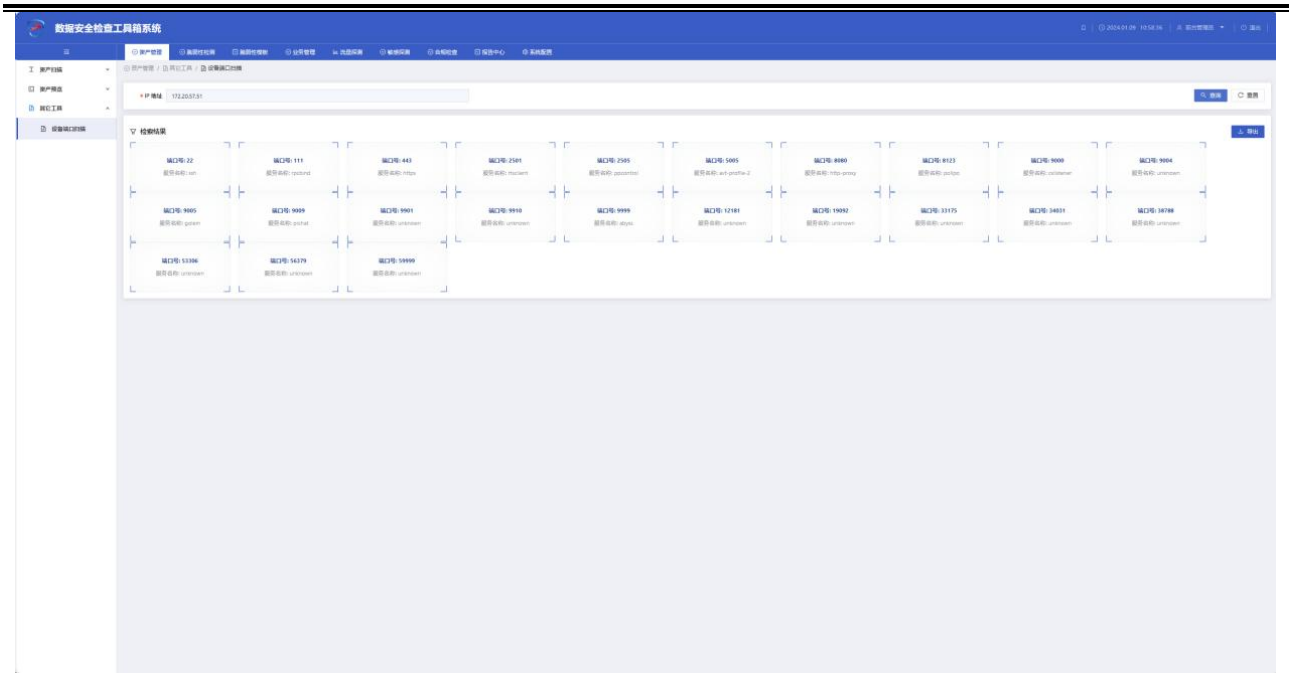


图 3.3.1 设备端口扫描

四. 脆弱性检测

任务中心为用户提供扫描任务扫描配置、任务下发、任务检测进度、任务检测结果的功能。

4.1 脆弱性检测包

新建任务模块主要是针对系统扫描、Web 扫描、口令猜解、仅做存活探测下发相应的扫描任务，分为基础配置和高级选项两大功能，对漏洞扫描结果有相应的描述、解决方法和检测详细。

4.1.1 基本配置

WEBUI：主界面 -> 脆弱性检测 -> 脆弱性检测包 -> 新建任务 -> 基本配置

基本配置页面是系统扫描，web 扫描，口令猜解，仅存活探测任务下发的统一入口，提供基础的扫描任务下发配置功能。

图 4.1.1 基本配置

基本配置参数说明如表 4.1.1 所示：

表 4.1.1 配置参数说明

参数	说明
新建任务类型	包括四种扫描类型：系统扫描，web 扫描，口令猜解，仅存活探测，如勾选仅存活探测，则不进行漏洞扫描，仅探测资产存活状态和端口开放情况
扫描目标方式	手动输入：针对系统扫描，web 扫描，口令猜解，仅做基础探测 4 中任务，扫描目标填写规范：IP，IP 段，域名或者 URL
	使用资产：针对系统扫描，web 扫描，口令猜解，仅做基础探测 4 中任务，扫描已生

	成的资产
	批量导入：针对系统扫描，web 扫描，口令猜解，仅做基础探测 4 中任务，以 Excel 的格式导入，减少工作量
	会话录制：仅针对 WEB 扫描，需要在会话录制页面提前录制好会话
扫描目标	被扫描对象，可以是 IP，IP 段，域名或者 URL，多个之间以英文逗号(,)或换行分隔： 1.IP 示例：192.168.1.100,2001:fecd:ba23:cd1f:dcb1:1010:9234:4088 2.IP 段示例： 192.168.1.0/24,192.168.2.1-254,192.168.3.1-192.168.3.254,192.168.1.* 3.域名示例：www.example.com 4.URL 示例： http://192.168.1.100/,https://www.example.com/,http://[2001:fecd:ba23:cd1f:dcb1:1010:9234:4088]/ 5.排除某个 IP：192.168.1.0/24!192.168.1.100
任务名称	可自定义，默认填充为扫描目标
执行方式	支持立即执行、定时执行和周期执行
漏洞插件模板	系统漏洞模板：仅选择系统扫描时展示，默认 7 种，可自定义，一般建议使用全部漏洞扫描模板
检测模式	WEB 漏洞插件模板：仅选择 web 扫描时展示，默认 3 种，可自定义，一般建议使用全部漏洞扫描模板
	口令猜解服务：仅选择口令猜解时展示，默认 36 种，选择口令猜解默认需要猜解服务类型。如需选择字典，请前往 -> 高级选项-> 口令猜解高级选项配置
	无：选择仅做存活探测的时候，没有展示
	可自定义扫描模式： 1.标准扫描：默认选择标准端口的端口范围，采用主机存活判断、端口 2.扫描、服务判断、漏洞测试的步骤对扫描目标进行完整的安全扫描。 3.快速扫描：快速的对扫描目标进行主机存活、端口服务探测。 4.完全扫描：默认选择全部端口的端口范围，采用主机存活判断、端口扫描、服务判断、漏洞测试的步骤对扫描目标进行完整的安全扫描。 5.深度扫描：利用配置好的用户名密码列表对主机进行登录后的安全扫描。
调试模式	默认不记录扫描执行日志，若开启将记录扫描执行日志。
分布式引擎	系统将根据引擎的负载情况，智能选择工作引擎，local：系统将会选择本地引擎
执行优先级	当任务达到并发上限时，’排队等待中’级别高的任务将优先执行
告警模板	是否需要扫描结束后向指定邮箱，手机用户，微信用户发送扫描结果，需提前在系统管理界面配置模板

4.1.2 高级选项

高级选项模块为系统扫描，web 扫描，口令猜解，仅做基础探测任务提供多元化的个性配置功能。

图 4.1.2 高级选项

4.1.2.1 系统扫描--登录信息选项

针对系统扫描，在提交系统扫描任务之前可对扫描目标进行登录验证，可单条添加，也可批量导入。如下图

图 4.1.2.1-1 系统扫描-登录验证

登录验证配置参数说明如表 4.1.2.1-1 所示：

表 4.1.2.1-1 配置参数说明

参数	说明
目标地址	可填入 IP：192.168.1.100 或者域名：www.example.com
服务	目前支持 8 种服务，SSH、SMB、TELNET、POP、POP3、IMAP、FTP、RDP
端口	登录端口号，整数，[1-65535]之间
用户名	主机登录的用户名
密码	主机登录的密码

4.1.2.2 系统扫描--探测选项

针对系统扫描，对扫描主机探测的配置功能。

图 4.1.2.2-1 系统扫描-探测选项

探测选项配置参数说明如表 4.1.2.2-1 所示：

表 4.1.2.2-1 配置参数说明

参数	说明
提示扫描目标	在扫描之前提示被扫描主机，需要扫描目标支持 messager 服务

4.1.2.3 系统扫描--检测选项

针对系统，高级配置扫描任务的个性化扫描需求。

图 4.1.2.3-1 系统扫描-检测选项

检测选项配置参数说明如表 4.1.2.3-1 所示

表 4.1.2.3-1 配置参数说明

参数	说明
最大限度报告漏洞	若选择关闭，则将大大提高扫描速率，部分耗时长的规则将跳过执行
执行所有规则检测	若选择开启：检测耗时越久、对检测目标的覆盖面更广
执行依赖插件	若选择开启：某些已例外的漏洞将加入到扫描结果当中
保存漏洞检测详情	若选择开启：漏洞的详细打印信息将加入到扫描结果当中

危险测试	包含一些危险的测试方法，如：拒绝服务检测，导致扫描目标的拒绝服务，因此慎用
停止探测无响应的主机	如果扫描过程中发现扫描目标没有反应，停止对该目标的探测
启用口令破解	使用默认字典对系统或服务的口令进行猜解
测试 Oracle 账号	对 Oracle 数据库进行深度检测

4.1.2.4 系统扫描--引擎选项

图 4.1.2.4-1 系统扫描-引擎选项

引擎选项配置参数说明如表 4.1.2.4-1 所示：

表 4.1.2.4-1 配置参数说明

参数	说明
插件超时	单个插件执行时间最长设置[10-300]
网络时延	网络连接超时设置[10-300]
单个主机检测并发数	针对单个的检测目标，并发的检测插件数量[1-50]
单个扫描任务并发主机数	单个扫描任务并发主机数
单个主机 TCP 连接数	针对单个检测目标，并发的 TCP 连接数量[1-1024]

4.1.2.5 系统扫描--其他配置

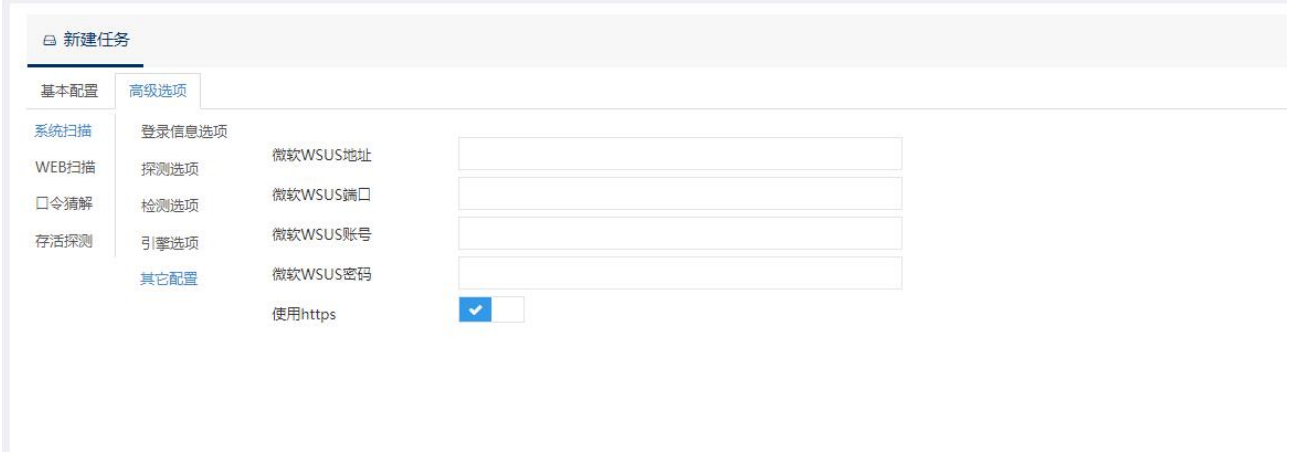


图 4.1.2.5-1 系统扫描-其他配置

4.1.2.6 WEB 扫描--登录扫描

针对 WEB 扫描任务，可对扫描任务进行登录配置

图 4.1.2.6-1 Web 扫描-登陆扫描

4.1.2.7 WEB 扫描--引擎配置

图 4.1.2.7-1 Web 扫描-引擎配置

Web 扫描-引擎配置配置参数说明如表 4.1.2.7-1 所示：

表 4.1.2.7-1 配置参数说明

参数	说明
并发线程数	单个扫描目标，并发执行的线程数量[1-50]
区分大小写	网站对于 Url 中字母大小写是否敏感
最大类似页面数	引擎用于归并类似链接时需要保留类似链接的数量[1-1000]
同目录下最大页面数	引擎在归并链接时，同一目录下需要保留的链接数量[1-1024]
重试次数	当链接无法访问时，重新访问的次数[1-10]
超时时间	当访问链接时超过多长时间，判定链接无法访问[1-300]
单个网站扫描超时设置	默认：0 无限制，单位：小时
代理类型	网站访问目标网站时，可能需要通过代理才能访问
静态 host 配置	引擎对域名的解析，多个域名与 IP 的对应关系以英文逗号(,)或换行分隔 域名与 IP 的对应格式示例：www.example.com 192.168.1.0 类似 192.168.3.cc、192.168.bb.cc、192.aa.bb.cc 格式将会被视为域名，请确认后提交

4.1.2.8 WEB 扫描--检测选项

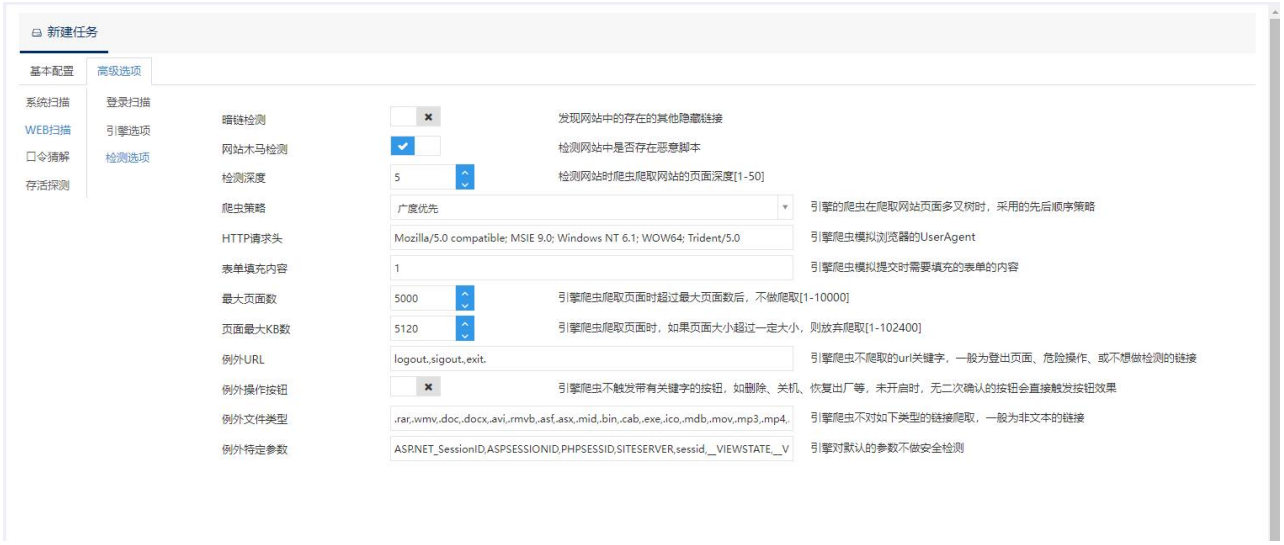


图 4.1.2.8-1 Web 扫描-检测选项

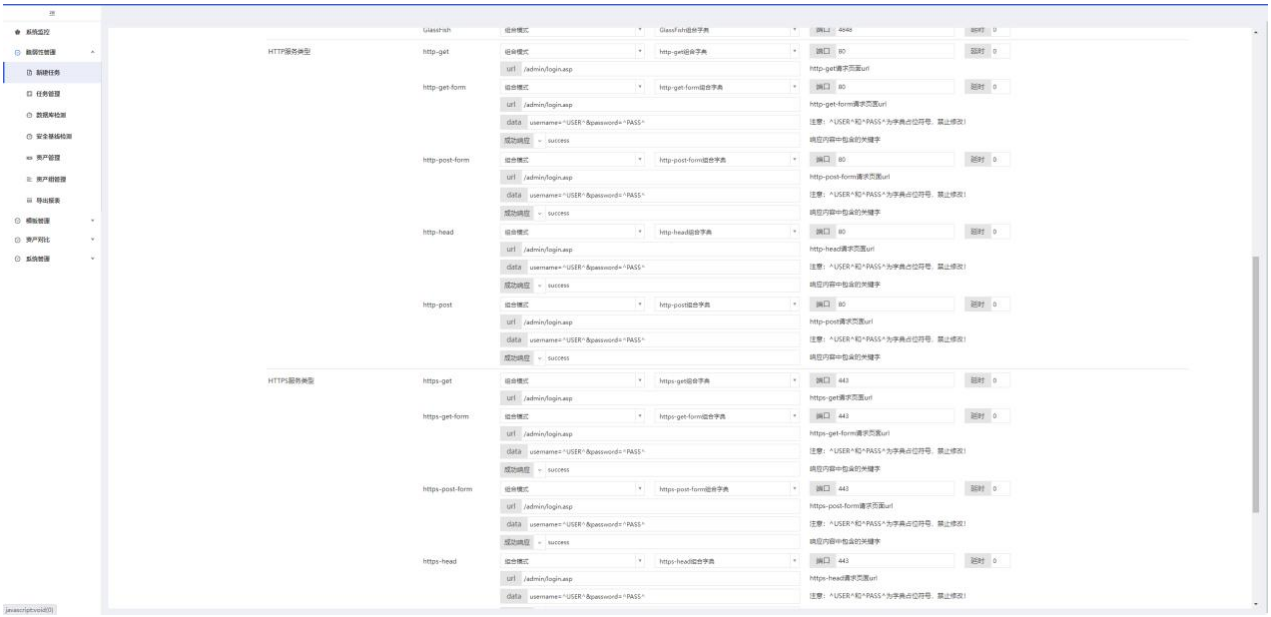
Web 扫描-检测选项配置参数说明如表 4.1.2.8-1 所示：

表 4.1.2.8-1 配置参数说明

参数	说明
暗链检测	发现网站中的存在的其他隐藏链接
网站木马检测	检测网站中是否存在恶意脚本

检测深度	检测网站中是否存在恶意脚本
爬虫策略	引擎的爬虫在爬去网站页面多叉树时，采用的先后顺序策略
Http 请求头	引擎爬虫模拟浏览器的 UserAgent
表单填充内容	引擎爬虫模拟提交时需要填充的表单的内容
最大页面数	引擎爬虫爬去页面时超过最大页面数后，不做爬取
页面最大 KB 数	引擎爬虫爬去页面时，如果页面大小超过一定大小，则放弃爬取
例外 URL	引擎爬虫不爬取的 url 关键字，一般为登陆页面、危险操作、或不想做检测的链接等
例外文件类型	引擎爬虫不对如下类型的链接爬取，一般为非文本的链接
例外特定参数	引擎对默认的参数不做安全检测

4.1.2.9 口令猜解--字典选择



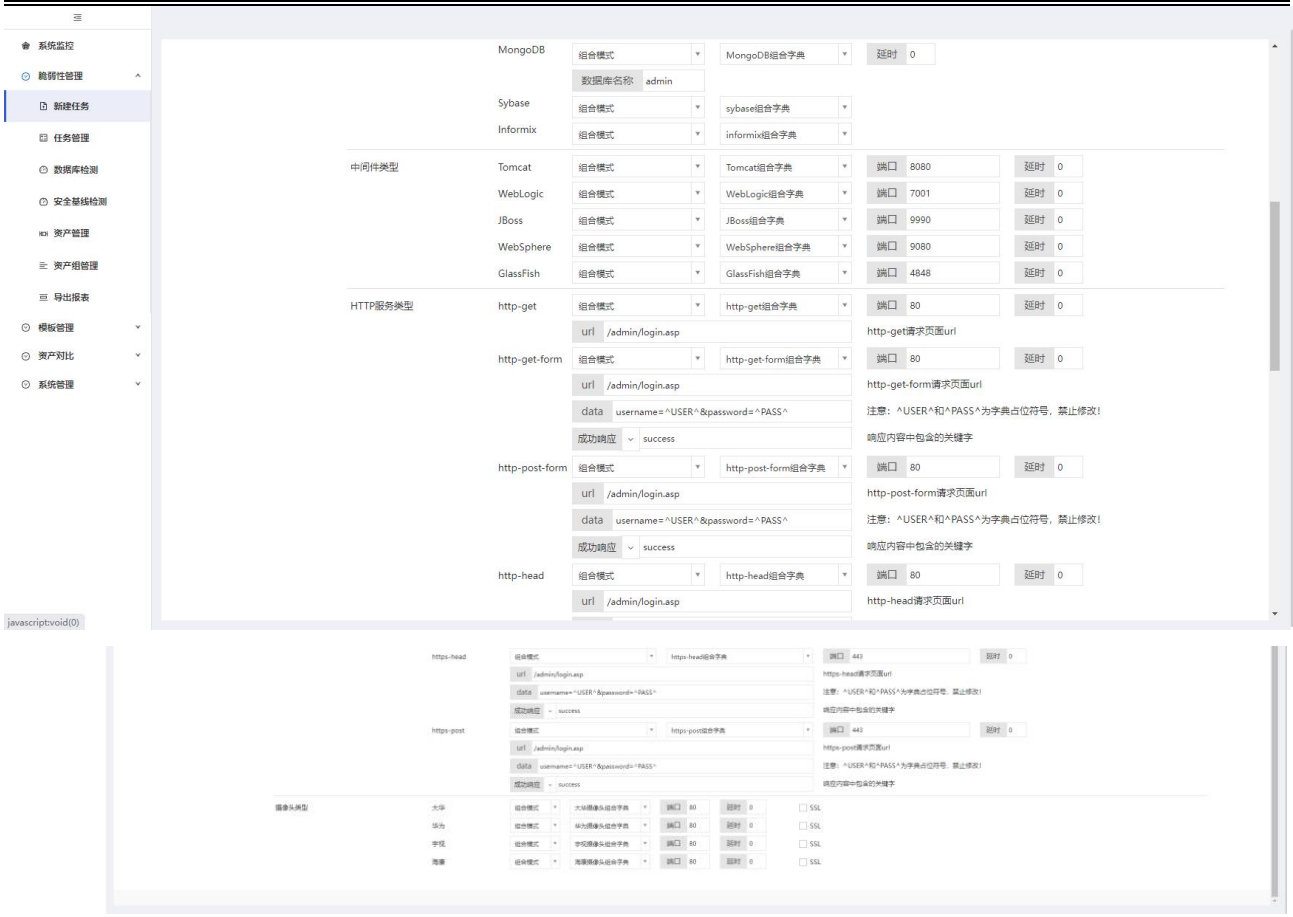


图 4.1.2.9-1 口令猜解--字典选择

字典选择配置参数说明如表 4.1.2.9-1 所示：

表 4.1.2.9-1 配置参数说明

参数	说明
服务类型	支持多种服务类型，字典可选用户名密码组合字典和标准字典，分别是“与”匹配和“或”匹配
数据库类型	支持多种数据库类型，字典可选用户名密码组合字典和标准字典，分别是“与”匹配和“或”匹配
中间件类型	支持多种中间件类型，字典可选用户名密码组合字典和标准字典，分别是“与”匹配和“或”匹配
HTTP 服务类型	支持多种 HTTP 服务类型，字典可选用户名密码组合字典和标准字典，分别是“与”匹配和“或”匹配
HTTPS 服务类型	支持多种 HTTPS 服务类型，字典可选用户名密码组合字典和标准字典，分别是“与”匹配和“或”匹配
摄像头类型	支持多种摄像头类型，字典可选用户名密码组合字典和标准字典，分别是“与”匹配和“或”匹配

4.1.2.10 口令猜解-引擎选项

图 4.1.2.10-1 口令猜--引擎选项

口令猜解—引擎选项配置参数说明如表 4.1.2.10-1 所示：

表 4.1.2.10-1 配置参数说明

参数	说明
最大线程并发数	对单个服务进行口令猜解的并发线程数，值越大，探测速度越快

4.1.2.11 存活探测--探测选项

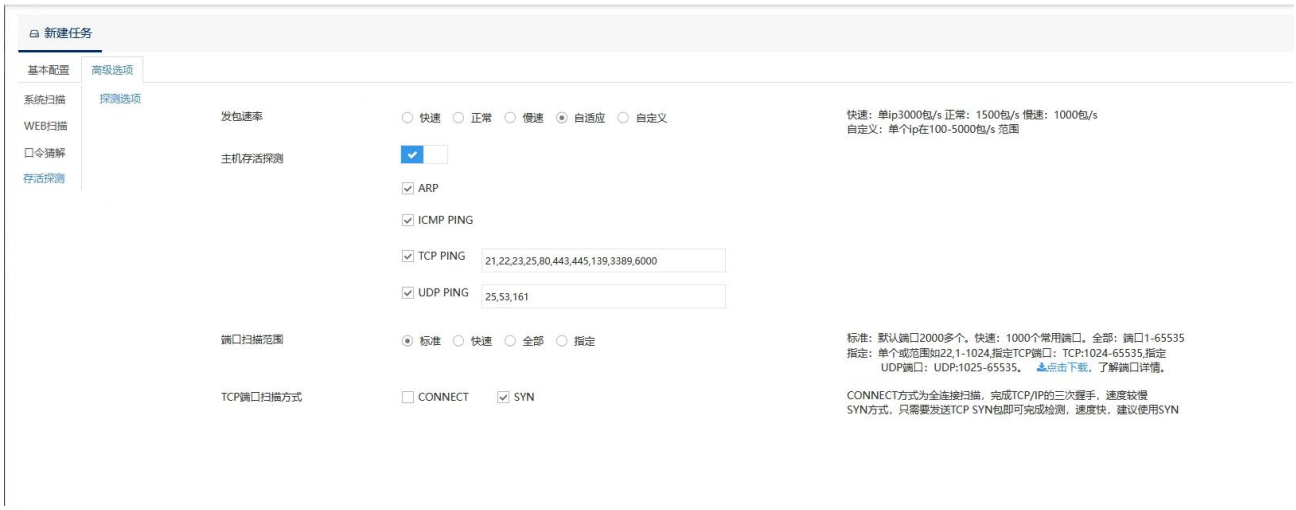


图 4.1.2.11-1 存活探测--探测选项

存活探测--探测选项配置参数说明如表 4.1.2.11-1 所示：

表 4.1.2.11-1 配置参数说明

参数	说明
发包速率	支持对发包速率的配置 1.快速：单 ip3000 包/s 2.正常：1500 包/s 3.慢速：1000 包/s 4.自定义：单个 ip 在 500-5000 包/s 范围

主机存活测试	对扫描主机的探测方式：ARP,ICMP PING,TCP PING,UDP PING ARP:通过 ARP 请求来实现探测，一般防火墙没法过滤 ARP 协议，成功率比 ICMP ping 高。 ICMP PING:测试网络的可达性和网络延迟。 TCP PING:使用 TCP 来向目标服务发送一个简单的 TCP 连接请求，等待服务器的响应。通常用来测试服务器是否在线和网络延迟。 UDP PING:使用 UDP 来向目标服务发送一个简单的 UDP 数据包，等待服务器的响应。通常用来测试网络质量和服务端的响应时间。 默认四个都勾选
端口扫描范围	1.标准：默认端口 4000 多个。 2.快速：100 个常用端口。 3.全部：端口 0-65535 4.指定：单个或范围如 22,1-1024，指定 TCP 端口：TCP:1024-65535,指定 UDP 端口：UDP:1025-65535
TCP 端口扫描方式	1.CONNECT 方式为全连接扫描，完成 TCP/IP 的三次握手，速度较慢 2.SYN 方式，只需要发送 TCP SYN 包即可完成检测，速度快，建议使用 SYN

4.2 任务管理

WEBUI：主界面 -> 脆弱性管理 -> 任务管理->任务列表

4.2.1 任务列表

任务列表模块主要展示全部的扫描任务，并可对扫描任务进行排序、查看、编辑、删除、以及按任务名称搜索等操作，也可实时且直观的查看任务扫描进度情况，以及对任务的执行操作，如立即执行、禁用等。如图 4.2.1-1 所示

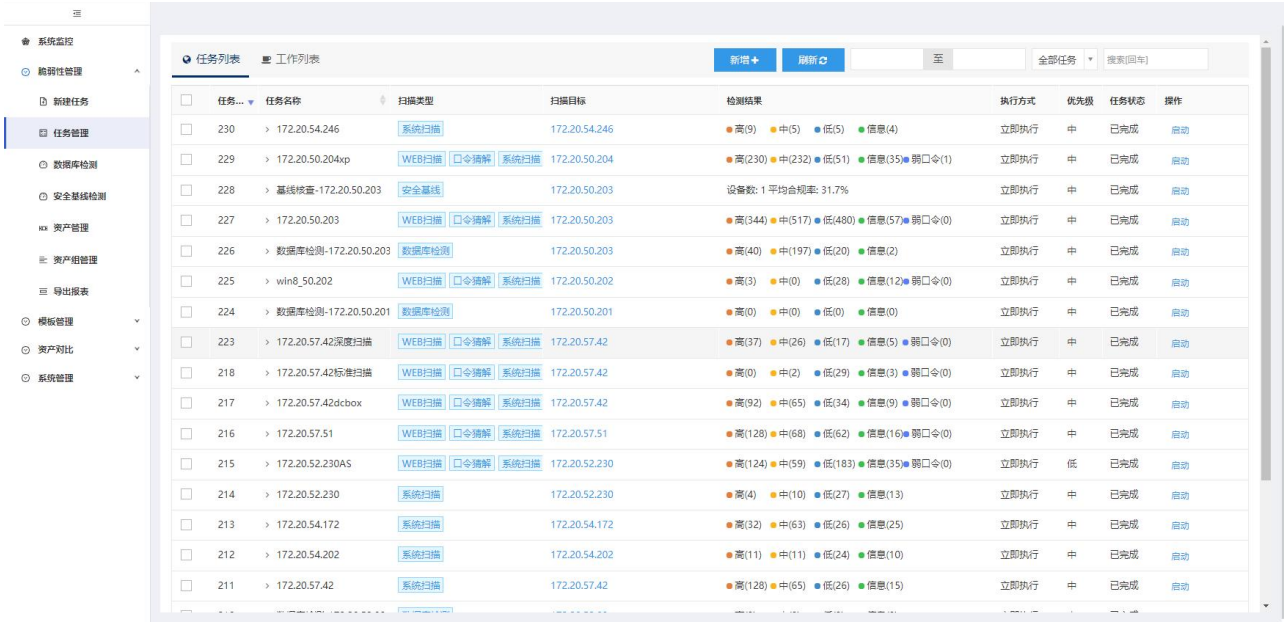


图 4.2.1-1 任务列表总览

任务列表总览配置参数说明如表 4.2.1-1 所示：

表 4.2.1-1 配置参数说明

参数	说明
任务名称	显示当前任务的名称，格式为用户在添加任务时的命名
执行方式	执行方式分为手动执行、定时执行、每日执行、每周执行、每月执行
扫描类型	显示当前任务的属于那种扫描任务，包含存活探测，WEB 扫描，口令猜解，系统扫描，数据库扫描，存活探测，安全基线
扫描目标	显示任务中所有的扫描目标
优先级	显示当前任务的优先级，有高中低三种
任务状态	包含排队等待，正在检测，已完成，已停止，已暂停，正在处理
检测结果	显示当前任务执行的进度情况，可以查看当前任务的高危，中危，低危，信息漏洞数，仅存活探测任务可以查看探测的存活主机数，基线任务可以查看设备数和平均合规率，口令猜解可以查看扫描的口令数
操作	可以选择立即开始或者禁用当前任务，对于正在执行的任务，可以选择暂停或者停止该任务

4.2.1.1 任务列表操作

任务扫描过程中可以对任务进行暂停、停止等操作，也可以对任务进行继续执行操作，如图所示：

图 4.2.1.1-1 扫描任务执行状态

4.2.1.2 扫描漏洞详情

系统扫描任务可展示：主机列表、漏洞列表、端口列表以及历史执行记录。点击漏洞列表可查看具体的漏洞详细信息，如图 4.2.1.2-1 所示：

图 4.2.1.2-1 系统扫描漏洞详情

点击漏洞会显示改漏洞的相应信息，编号、风险级别、年份、描述、解决方法、检测详细等，如图 4.2.1.2-2 所示：

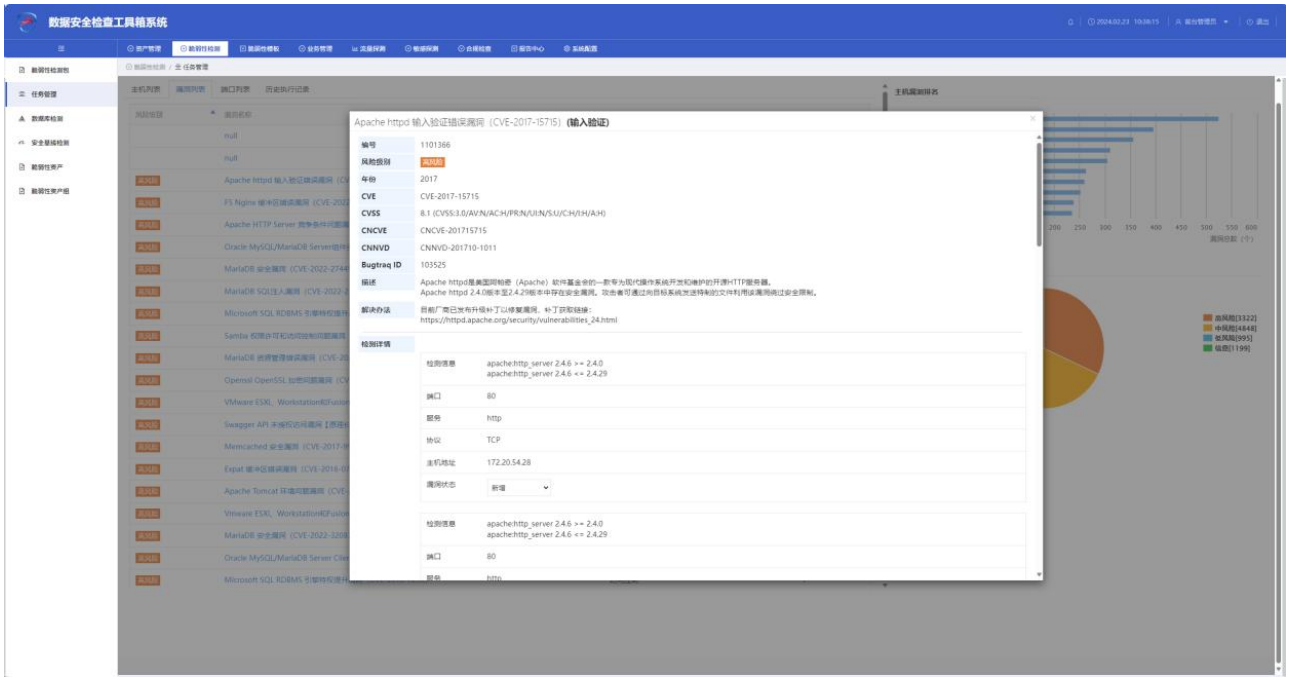


图 4.2.1.2-2 漏洞详情

Web 扫描任务可显示：主机列表、漏洞列表、漏洞目录树以及历史执行记录。点击网站目录结构，可查看漏洞目录树以及对应的漏洞详情，如图 4.2.1.2-3 所示：

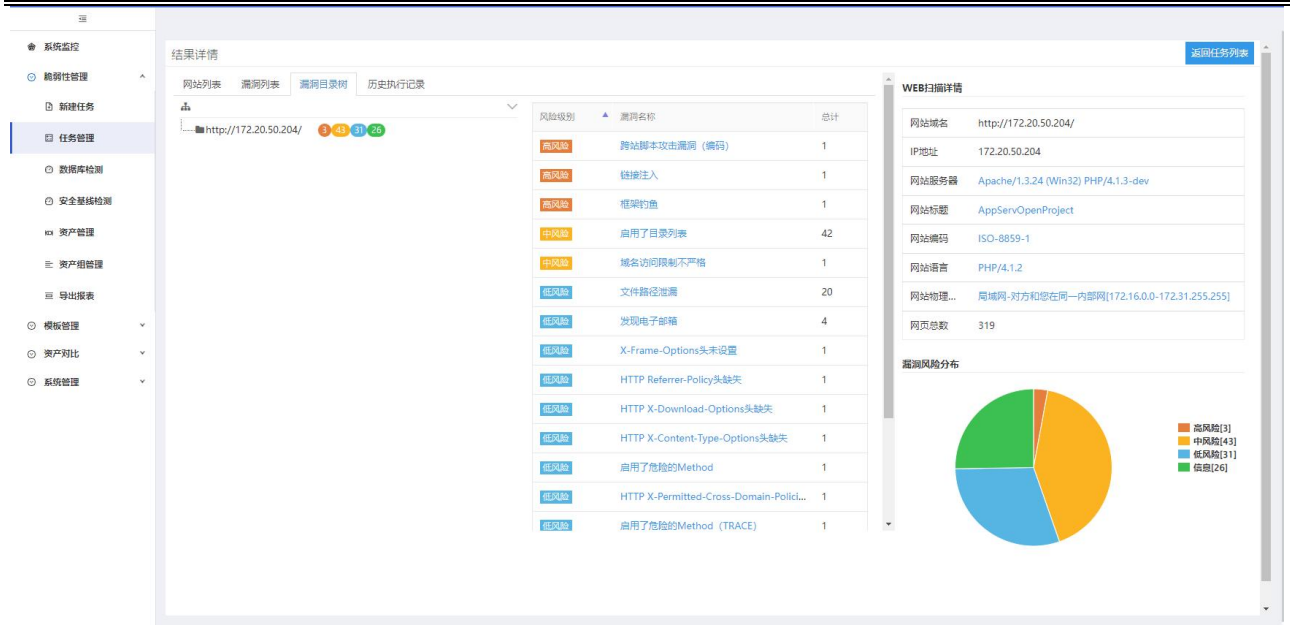


图 4.2.1.2-3 Web 扫描漏洞详情

点击漏洞列表中的漏洞，显示该漏洞的相关信息，并可以对其进行验证操作，如图 4.2.1.2-4 所示：

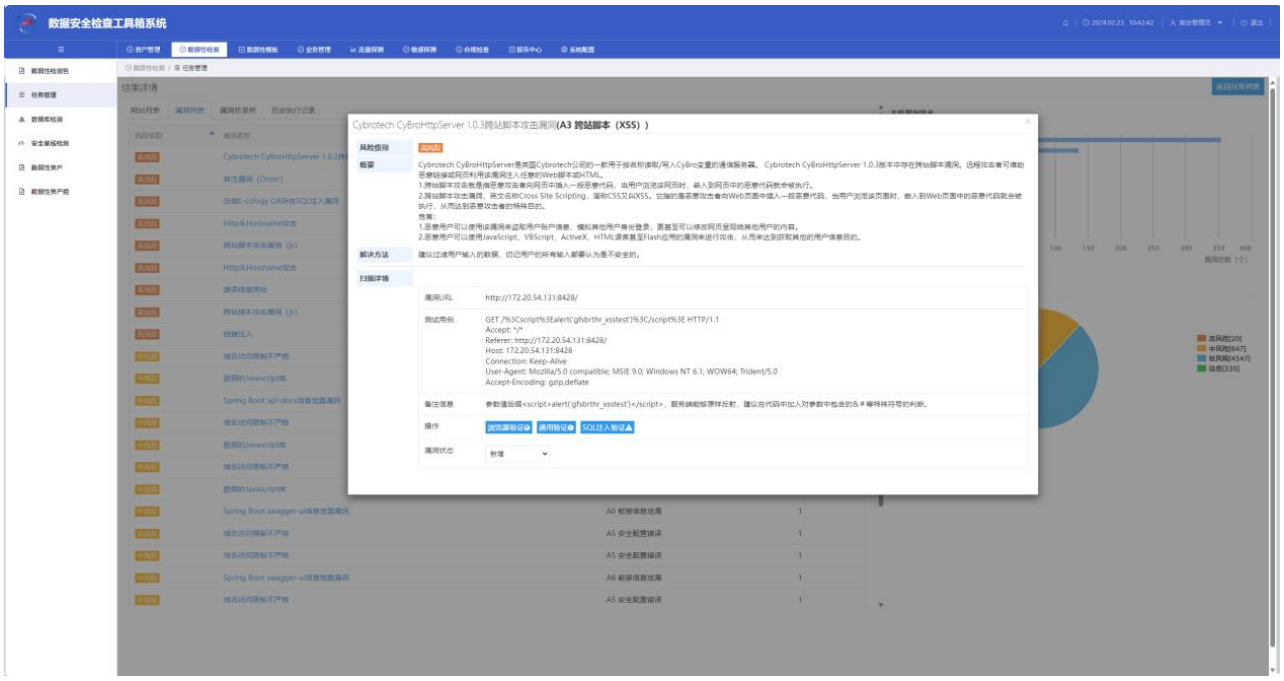


图 4.2.1.2-4 漏洞详细

口令猜解任务可显示：主机列表、弱口令列表以及历史执行记录，如图 5.2.1.2-5 所示：

图 4.2.1.2-5 弱口令列表

仅存活探测任务可显示：主机列表、以及历史执行记录，如图 4.2.1.2-6 所示

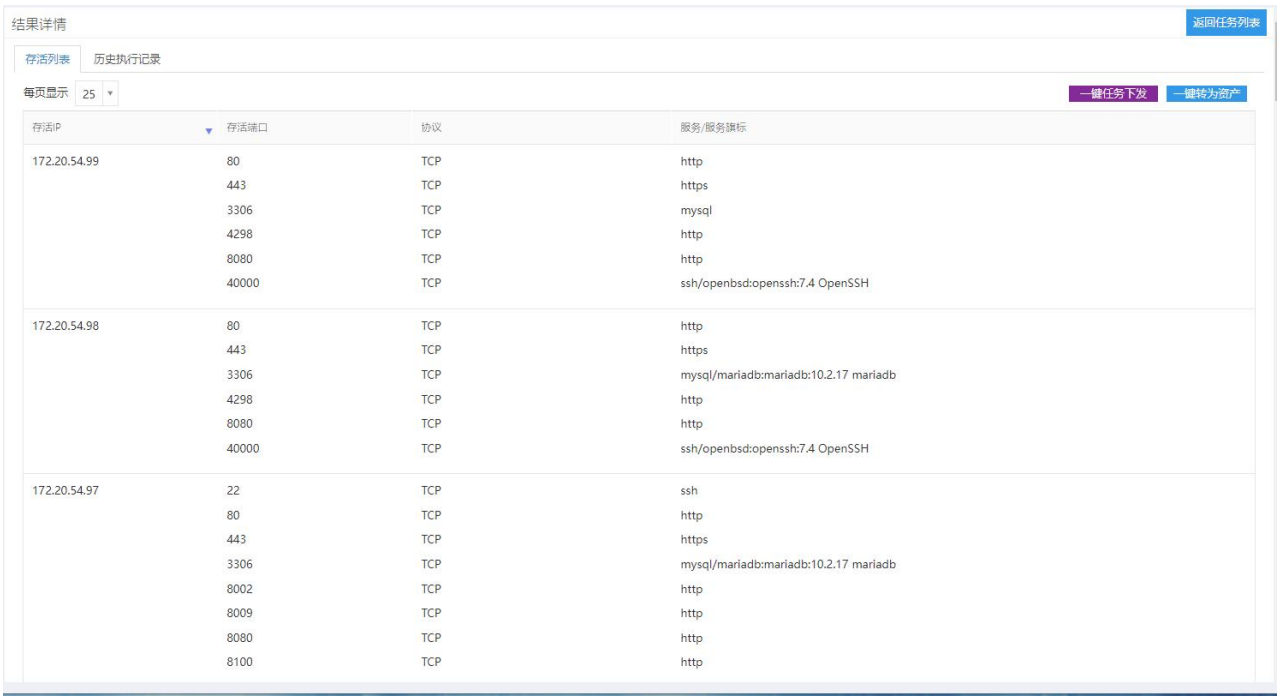


图 4.2.1.2-6 存活列表

仅基线可显示：主机列表、核查项，以及历史执行记录，如图 4.2.1.2-7 所示

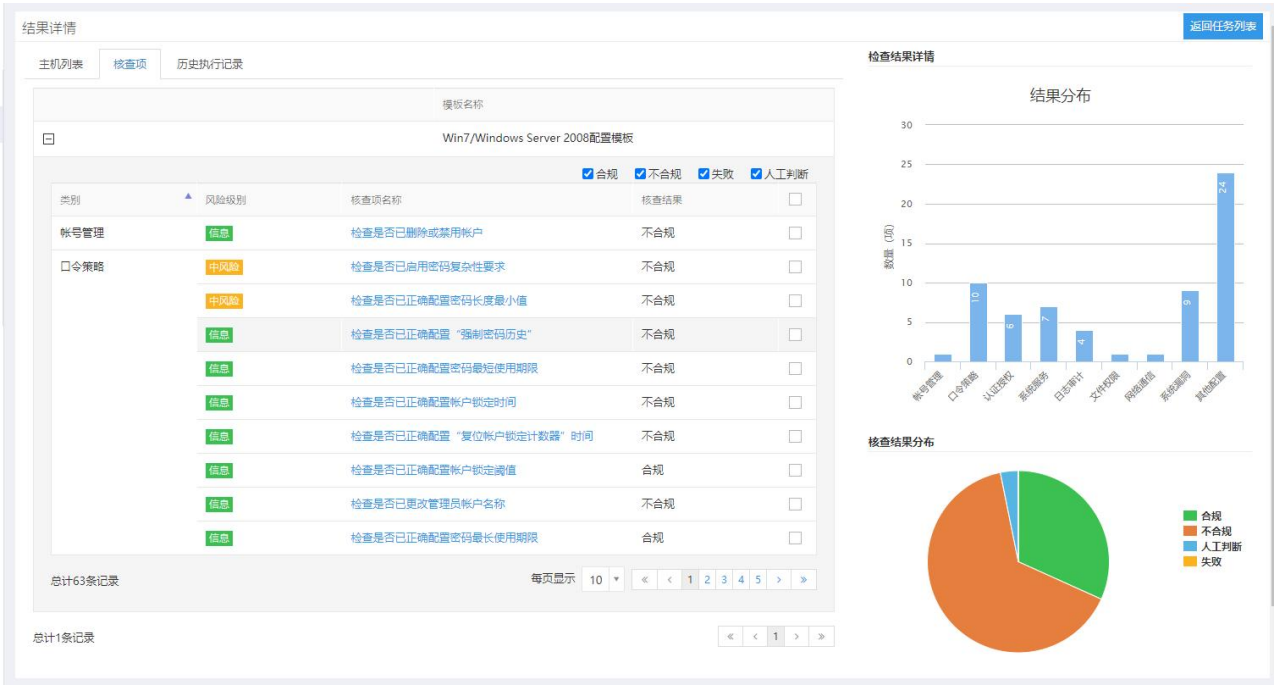


图 4.2.1.2-7 安全基线

4.2.1.3 任务状态控制

➢立即执行

在任务列表点击操作栏的【立即执行】，将已完成或者尚未执行的任务立即启动执行

➢禁用

在任务列表点击操作栏的【禁用】，周期任务将不随周期执行，点击【启用】后，周期任务可正常跟随周期执行

➢**停止**

在任务列表点击操作栏的【停止】，将正在执行的任务全部停止，任务不再执行，点击立即执行后，任务会重新下发进行执行

➢**暂停**

在任务列表点击操作栏的【暂停】，将正在执行的任务暂停，点击【继续】，暂停的任务会接着暂停前的进度继续执行，不会重新下发

4.2.1.4 编辑任务

操作：（1）在任务列表页面，选择任务->点击【编辑】，跳转到任务配置页面，对任务配置进行修改，任务名称和扫描目标不支持编辑，如下

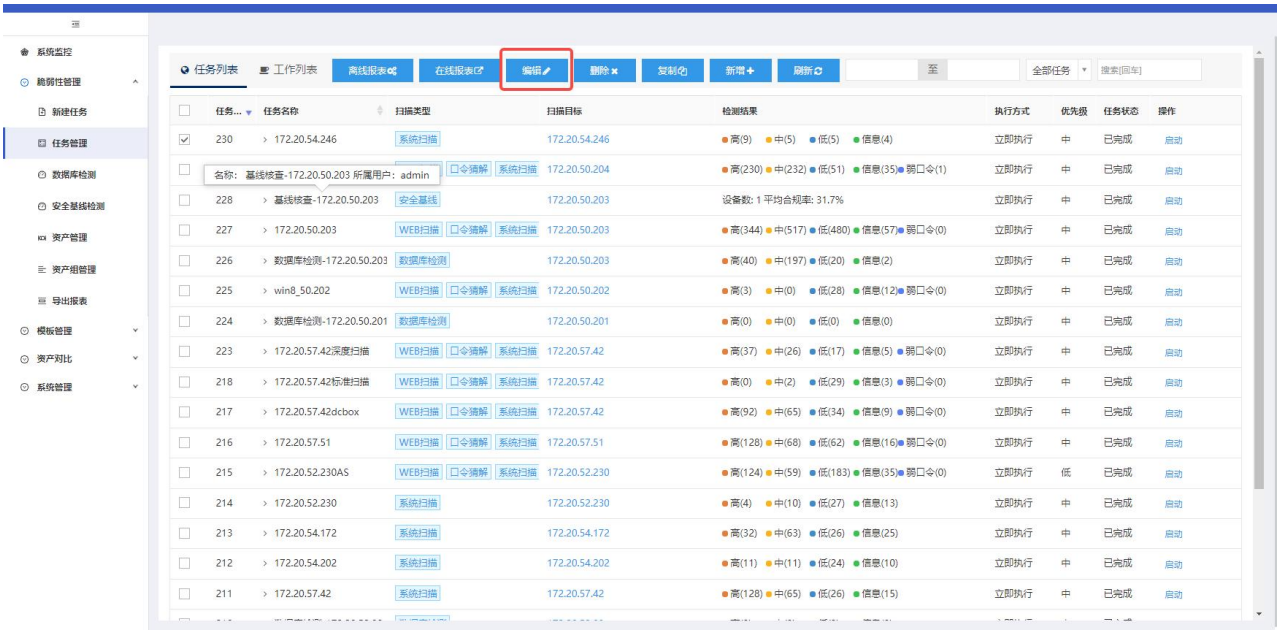


图 4.2.1.4-1 编辑任务

（2)修改任务配置后点击【提交】，任务重新执行时会按照修改后的配置进行扫描

4.2.1.5 删除任务

操作：（1）在任务列表页面，选择任务->点击【删除】->确认，即可将所选任务删除，任务删除后，任务生成的资产不会被删除，但是该资产就无法导出报表

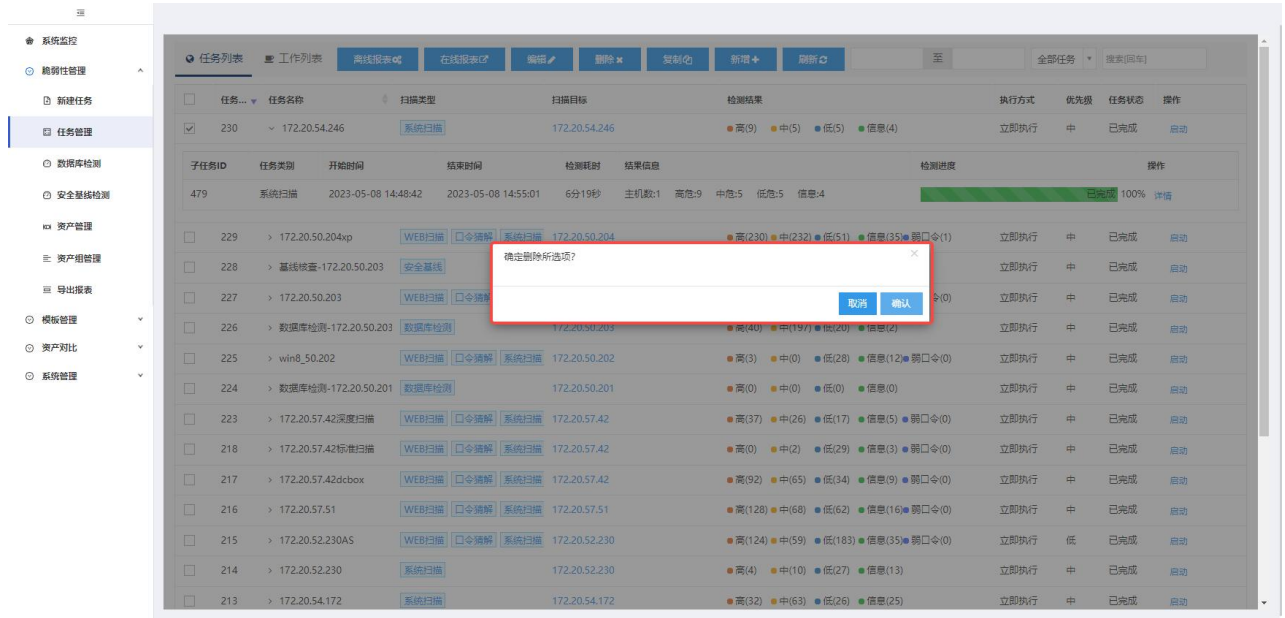


图 4.2.1.5-1 删除任务

4.2.1.6 复制任务

复制任务是复制任务的配置信息，需输入扫描目标和任务名称

操作：（1）在任务列表页面，选择任务->点击【复制】->弹窗显示复制任务的输入框，

如下

图 4.2.1.6-1 复制任务目标输入

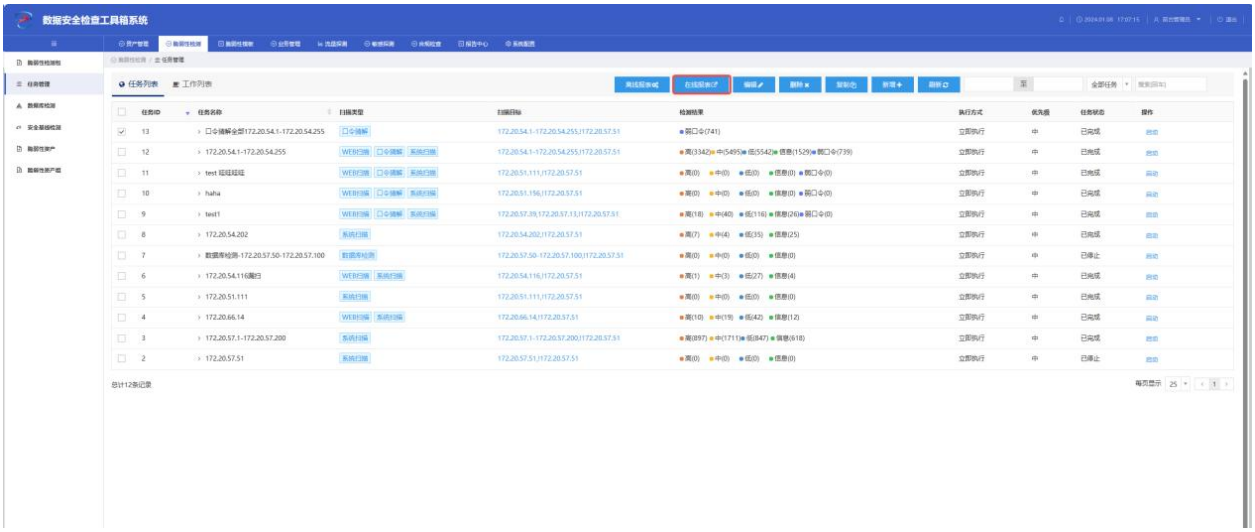
（2）输入扫描目标和任务名称后点击【提交】，即可在任务列表生成任务

图 4.2.1.6-2 复制任务

4.2.1.7 查看任务在线报表

只有经过系统扫描、web 扫描或者口令猜解的任务可查看在线报表，若任务尚未执行或者任务类型是仅存活探测任务，则无法查看在线报表

操作：（1）在任务列表页面，选择任务->点击【在线报表】，直接自动新建标签页进入任务的统计报表页面，即可查看该任务的统计报表，如下




漏洞扫描安全评估报告

目录
1 检测结果综述
2 任务总体概览
2.1 任务基本信息
2.2 敏感端口/服务
2.3 敏感中间件
3 资产信息统计
3.1 端口/服务统计
3.2 资产风险等级
3.2.1 主机资产风险
3.2.2 WEB资产风险
4 漏洞信息统计
4.1 受影响资产统计
4.1.1 系统漏洞影响资产
4.1.2 WEB漏洞影响资产
4.2 漏洞等级分布
4.3 漏洞类别统计
4.3.1 系统漏洞类别
4.3.2 WEB漏洞类别
4.4 漏洞排名
4.4.1 系统漏洞TOP10
4.4.2 WEB漏洞TOP10
5 弱口令
6 历史检测详情
7 参考标准
7.1 单一漏洞风险等级评定标准
7.2 资产风险等级评定标准
8 安全建议
9 联系我们

1 检测结果综述

本次检测中，扫描了1个主机，0个站点。
检测到漏洞共23个，系统漏洞23个，Web漏洞0个。高危漏洞共9个，中危漏洞共5个，低危漏洞共5个，信息级漏洞共4个。
检测到弱口令共0个。
整体风险等级为 非常危险，非常危险的资产共1个，需重点关注。

2 任务总体概览

2.1 任务基本信息

任务名称	172.20.54.246
扫描目标	172.20.54.246
报表模板	默认模板
任务所在账号	admin
扫描时间	系统扫描：2023-05-08 14:48:42 至 2023-05-08 14:55:01（耗时：6分19秒）
系统版本	V3.0(6.6.1-R1-v90757-20230222)
规则库版本	20230324144746

2.2 敏感端口/服务

本次任务检测到开放了以下【2】种敏感端口或服务，开放最多的端口为【80】端口，对应【1】个资产，具体情况如下表所示。

序号	端口	服务	协议	主机
1	80	vmware esxi server/http/VMware ESXi Server httpd	TCP	172.20.54.246
2	443	https	TCP	172.20.54.246

说明：敏感端口/服务指根据安全研究表明，容易被黑客利用漏洞发起攻击的端口/服务。

2.3 敏感中间件

本次任务检测到以下种敏感中间件，其中使用最多的中间件是【】，具体情况如下表所示：

序号	中间件	网站

说明：敏感中间件是指安全研究表明，容易被黑客利用发起攻击的中间件。

3 资产信息统计

3.1 端口/服务统计

资产的端口/服务开放情况如下表所示，开放端口最多的资产为【172.20.54.246】，共开放了【7】个端口：

序号	主机名	端口/"服务"/协议	端口总数

图 4.2.1.7-1 在线报表-统计报表

（2）点击统计报表里【2.2 整体漏洞统计】章节的 IP（域名），直接新开标签页跳转到所点击资产的详细报表页面，即可查看所点击资产的详细报表


2.2 整体漏洞统计

以IP为维度，覆盖主机IP以及该IP上存在的Web站点，整体进行漏洞统计，统计结果如下表所示：

序号	IP（域名）	高	中	低	信息	总计（次）
1	172.18.0.252	6	1	4	0	11

2.3 敏感端口/服务 转到详细报表

1 检测结果综述

本次报告中，目标【172.18.0.252】共检测出风险11个，其中系统漏洞0个，Web漏洞11个，弱口令0个。

整体风险值为6.6，安全等级为比较危险。所有漏洞中，高危漏洞6个，中危漏洞1个，低危漏洞4个，信息级漏洞0个。（漏洞风险等级的分类规则及资产风险等级分类规则，请参见章节《资产风险等级评定标准》）。

2 资产总体概览

2.1 资产基本信息

系统资产列表：

WEB资产列表：

Web资产	http://172.18.0.252:10007/
网站域名	172.18.0.252
IP地址	172.18.0.252
服务器信息	
网站标题	S2-053Demo
网站编码	UTF-8
服务器语言	
网站物理地址	
扫描时间	开始时间：【2020-06-24 06:43:48】结束时间：【2020-06-24 06:50:35】(耗时：6分47秒)
资产风险值	6.6
漏洞分布	漏洞总计：11 高风险：6 中风险：1 低风险：4 信息：0
漏洞状态标识	新增：11 误报：0 已修复：0
资产组	zx-webscan

图 4.2.1.7-2 在线报表-详细报表

➢在线报表导出到本地

操作：点击在线报表右上方的  ，即可将任务报表导出到本地

4.2.2 工作列表

WEBUI：主界面 -> 任务中心 -> 任务列表->工作列表

工作列表主要展示了当前开启的任务中正在执行的任务。可以看到该任务的任务名称，开始时间，检测耗时以及执行的进度。也可以对正在执行的任务进行停止或强制停止操作，也可以对工作列表进行排序、搜索等。具体界面如图 5.2.2-1 所示：

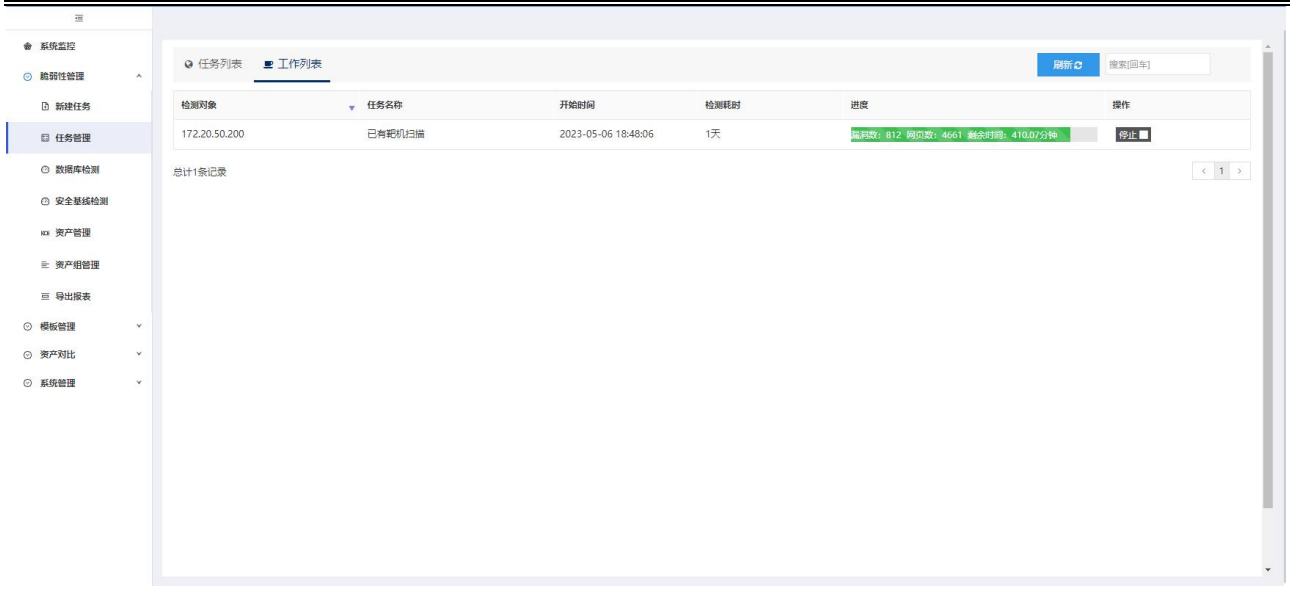


图 4.2.2-1 工作列表

工作列表各项参数说明如表 4.2.1-1 所示：

表 4.2.1-1 各项参数说明

参数	说明
检测对象	显示当前任务中里包含的检测对象
任务名称	显示当前任务的名称，格式为用户在添加任务时的命名
开始时间	显示当前评估任务的开始时间
检测耗时	可以实时的展示出任务执行检测大致需要的执行时间，执行完成会显示整个任务扫描花费的时长
进度	显示当前任务执行的进度情况，如果是 web 扫描可以展示漏洞数，网页数，剩余时间，如果是系统扫描会展示漏洞数，主机数，剩余时间
操作	对于正在执行的任务，可选择停止/强制停止当前任务

⚠注意： 工作列表中的进度条显示的是单个任务的单个检测目标，一个任务可包含多个扫描目标，相应的也会有多个工作列表。

4.3 数据库检查

WEBUI：主界面 -> 任务中心 -> 数据库检查

4.3.1 检测基本配置

针对数据库扫描，添加需要扫描的目标，填写形式为单个主机或者主机组，配置任务名称，选择数据库扫描插件模板并提交扫描。具体如下图 4.3.1-1 所示：

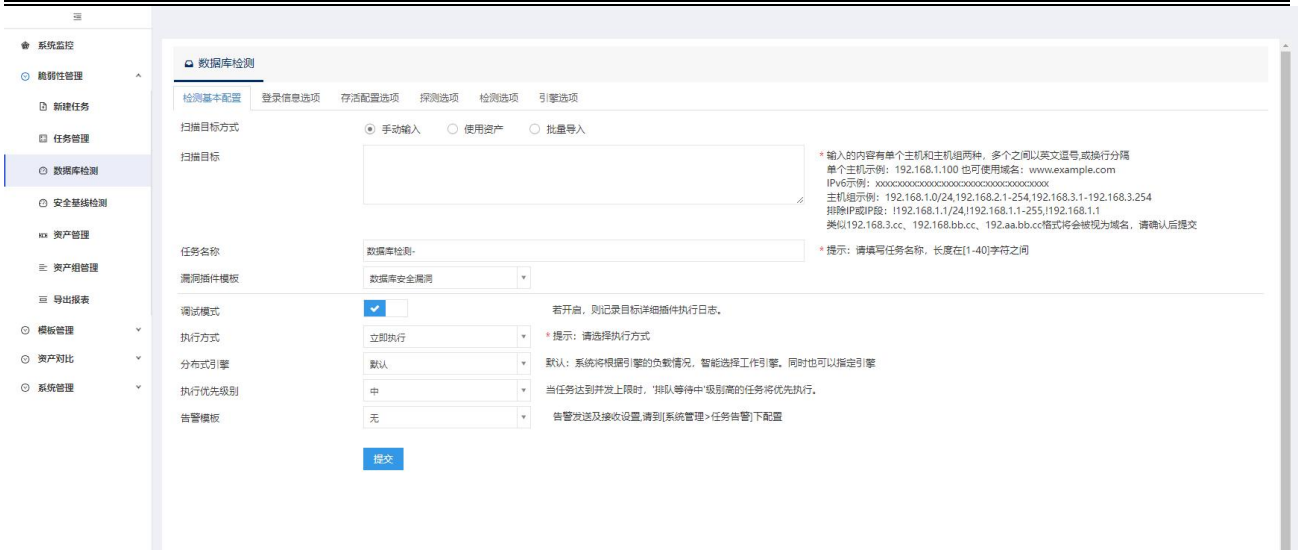


图 4.3.1-1 新建数据库扫描任务

新建数据库扫描任务配置参数说明如表 4.3.1-1 所示：

表 4.3.1-1 配置参数说明

参数	说明
扫描目标方式	1.手动输入：可输入单个主机或主机组，即扫描对象
	2.使用资产：扫描已知资产，资产管理界面需要有资产
	3.批量导入：以 Excel 的格式导入，减少工作量
扫描目标	被扫描对象，可以是单个主机或主机组 1. 输入的内容有单个主机和主机组两种，多个之间以英文逗号,或换行分隔 2. 单个主机示例：192.168.1.100 也可使用域名：www.example.com 3. IPv6 示例：2001:fecd:ba23:cd1f:dcb1:1010:9234:4088 4. 主机组示例：192.168.1.0/24,192.168.2.1-254,192.168.3.1-192.168.3.254 5. 排除某个 IP：192.168.1.0/24!192.168.1.100
任务名称	可自定义，默认前缀是为了区分不同的扫描任务
执行方式	支持立即执行、定时执行和周期执行
漏洞插件模板	选择数据库漏洞插件模板
调试模式	默认不记录扫描执行日志，若开启将记录扫描执行日志。
执行优先级	当任务达到并发上限时，’排队等待中’级别高的任务将优先执行。可选择高/中/低
分布式引擎	是否作为分布式扫描引擎工作，常规扫描‘默认’即可
告警模板	告警发送及接收设置,请到[系统管理>任务告警]下配置

4.3.2 登录信息选择

可对扫描任务靶机进行登录验证。

图 4.3.2-1 数据库扫描-登录验证

4.3.3 存活配置选项

可对扫描任务靶机进行存活验证。

图 4.3.3-2 数据库扫描-登录验证

数据库扫描-存活配置选项参数说明如表 4.3.4-1 所示：

参数	说明
发包速率	支持对发包速率的配置 1.快速：单 ip3000 包/s 2.正常：1500 包/s 3.慢速：1000 包/s 4.自定义：单个 ip 在 500-5000 包/s 范围
主机存活测试	对扫描主机的探测方式：ARP,ICMP PING,TCP PING,UDP PING ARP:通过 ARP 请求来实现探测，一般防火墙没法过滤 ARP 协议，成功率比 ICMP ping 高。 ICMP PING:测试网络的可达性和网络延迟。 TCP PING:使用 TCP 来向目标服务发送一个简单的 TCP 连接请求，等待服务器的响应。通常用来测试服务器是否在线和网络延迟。

	UDP PING:使用 UDP 来向目标服务发送一个简单的 UDP 数据包，等待服务器的响应。通常用来测试网络质量和服务端的响应时间。 默认四个都勾选
端口扫描范围	1.标准：默认端口 4000 多个。 2.快速：100 个常用端口。 3.全部：端口 0-65535 4.指定：单个或范围如 22,1-1024，指定 TCP 端口：TCP:1024-65535,指定 UDP 端口：UDP:1025-65535
TCP 端口扫描方式	1.CONNECT 方式为全连接扫描，完成 TCP/IP 的三次握手，速度较慢 2.SYN 方式，只需要发送 TCP SYN 包即可完成检测，速度快，建议使用 SYN

4.3.4 探测选项

图 4.3.4-1 数据库扫描-探测选项

数据库扫描-探测选项配置参数说明如表 4.3.4-1 所示：

表 4.3.4-1 配置参数说明

参数	说明
提示扫描目标	在扫描之前提示被扫描主机，需要扫描目标支持 messager 服务

4.3.5 检测选项

图 4.3.5-1 数据库扫描-检测选项

数据库扫描-检测选项配置参数说明如表 4.3.5-1 所示：

表 4.3.5-1 配置参数说明

参数	说明
最大限度报告漏洞	若选择关闭，则将大大提高扫描速率，部分耗时长的规则将跳过执行
执行所有规则	若选择开启：检测耗时越久、对检测目标的覆盖面更广
危险测试	包含一些危险的测试方法，如：拒绝服务检测，导致扫描目标的拒绝服务，因此慎用
启用口令破解	使用默认字典对系统或服务的口令进行猜解
测试 Oracle 账号	对 Oracle 数据库进行深度检测

4.3.6 引擎选项

图 4.3.6-1 数据库扫描-引擎选项

数据库扫描-引擎选项配置参数说明如表 4.3.6-1 所示：

表 4.3.6-1 配置参数说明

参数	说明
插件超时	单个插件执行时间最长设置[10-300]
单个主机检测并发数	针对单个的检测目标，并发的检测插件数量[1-50]
单个扫描任务并发主机数	单个扫描任务并发主机数
单个主机 TCP 连接数	针对单个检测目标，并发的 TCP 连接数量[1-1024]

4.4 安全基线检测

安全基线检测采用机器语言，模拟人访问 IT 资产的全过程，自动化的采集各 IT 资产的安全配置，并对安全配置信息进行自动化解析，与安全知识库中的安全配置要求及基准点进行比对，以检查安全配置符合情况，自动化出具丰富详实的核查报告。

安全基线扫描可针对基线核查任务进行编辑、删除、排序等，可以根据列表显示查看到任务名称、扫描策略、开始时间、结束时间和扫描进度；启动按钮可以重新复制任务扫描基线；在线报表可以查看基线扫描结果详情。具体如下图 5.4.1 所示：

图 4.4 基线核查任务列表

4.4.1 在线任务-检测基本配置

新建在线的基线检测任务：针对在线检测任务，输入目标、任务名称，选择扫描策略，配置登录信息和核查的模板类别并配置其他选项提交任务。如图 4.4.1 所示：

图 4.4.1-1 新建基线核查任务

新建基线核查任务配置参数说明如表 4.4.1 所示：

表 4.4.1 配置参数说明

参数	说明
创建任务方式	1.在线任务：下发任务时配置好目标主机的登录信息，系统远程访问进行检测 2.离线任务：将离线模板下载到目标主机上，在目标主机上检测完后后将结果导入系统进行结果查询
扫描目标方式	手动输入：可输入单个主机或主机组
	使用资产：扫描已知资产，需先在【资产管理】下添加
	批量导入：以 Excel 的格式导入，减少工作量
检测目标	输入的内容有单个主机和主机组两种，多个之间以英文逗号,或换行分隔 1.单个主机示例：192.168.1.10 2.主机组示例：192.168.1.1-192.168.1.10 范围不超过 255 个
任务名称	输入基线扫描任务的任务名称
扫描策略	根据客户自己行业性质、单位要求标准等选择所需的扫描策略

●设备列表配置：设备列表用来展示并配置目标主机登录信息和选择检测模板，如下图 4.4.1-2

图 4.4.1-2 设备列表

●设备列表生成方式有两种：

（1）手动输入或者导入，IP 地址由扫描目标自动生成，点击操作栏的【编辑】手动配置目标主机登录信息和检测模板;如下图 4.4.1-3

图 4.4.1-3 编辑设备信息

（2）使用已检测过的资产，下拉选择历史任务和检测时间，直接继承旧任务的配置信息，如下图 3.4.1-4

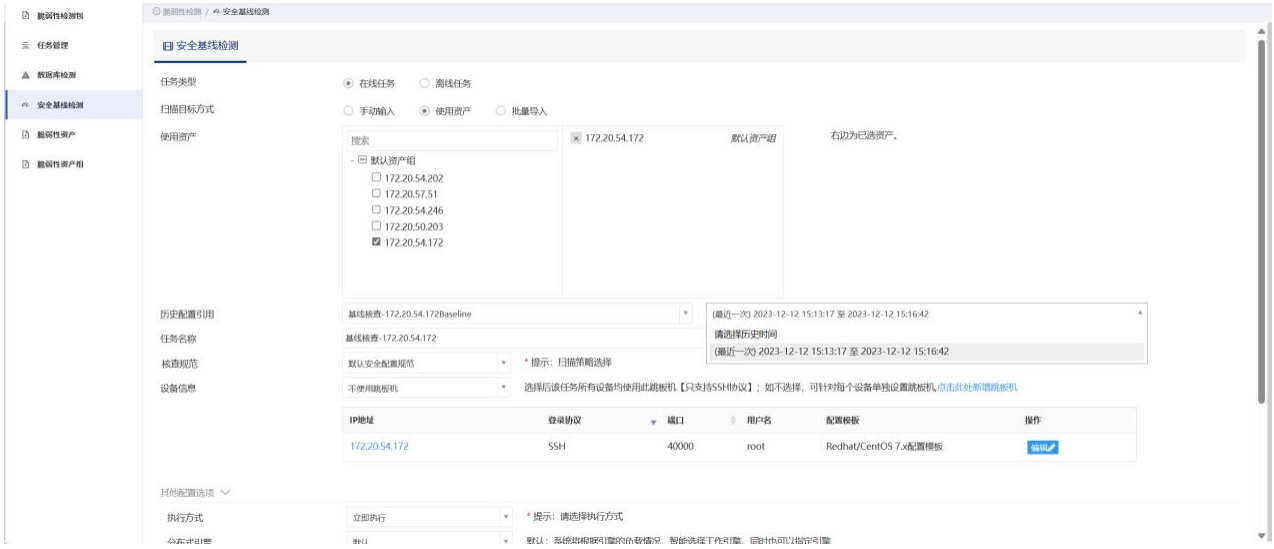


图 4.4.1-4 选择历史配置信息

基线检测目标主机信息配置和模板选择参数说明如下表 4.4.1-2：

表 4.4.1-2 设备列表配置参数表

参数	说明
编辑设备	登录目标主机所需的协议、端口、账号、密码，目前支持协议有：SSH、Telnet、RDP、SMB、WinRM
设备模板	根据目标主机的操作系统、设备类型选择对应的设备模板
数据库配置模板	根据所选的设备模板，自动列出对应数据库配置模板. 输入数据库配置模板相对应的配置. 示例:mysql 数据配置 /usr/bin/mysql
应用服务器模板	根据所选的设备模板，自动列出对应应用服务器配置模板. 输入应用服务器配置模板相对应的配置. 示例: WebSphere 配置 /opt/IBM/WebSphere/AppServer_1/
登陆验证	测试对应协议登陆主机用户名及密码是否正确，协议所选是否支持

4.4.2 离线任务-检测基本配置

离线任务：将在目标靶机上执行的基线核查结果导入到系统，直接进行解析和结果查看，没有远程登录和检测的过程，创建离线任务如下图 4.4.2-1：

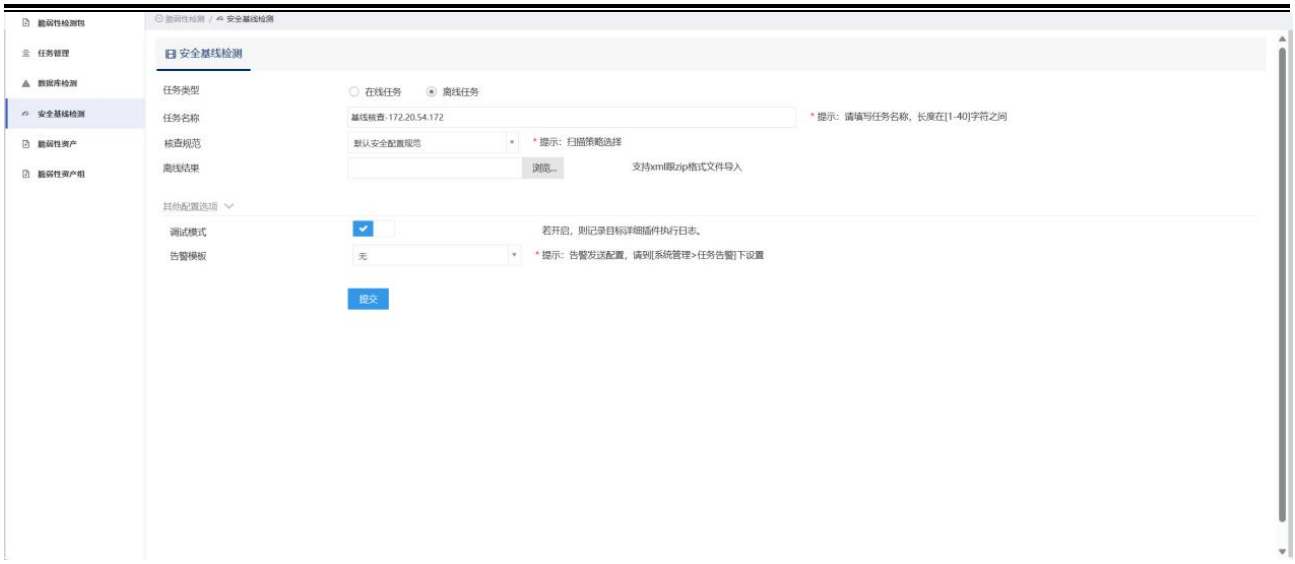


图 4.4.2-1 选择历史配置信息

离线任务配置参数说明见下表 4.4.2-1：

表 4.4.2-1 ；离线任务配置参数表

参数	说明
创建任务方式	1.在线任务：下发任务时配置好目标主机的登录信息，系统远程访问进行检测 2.离线任务：将离线模板下载到目标主机上，在目标主机上检测完后后将结果导入系统进行结果查询
任务名称	输入基线扫描任务的任务名称
扫描策略	根据客户自己行业性质、单位要求标准等选择所需的扫描策略。
离线结果	将在目标靶机上执行的结果导入到系统，支持 zip 和 xml 格式，错误的文件无法解析

⚠ 备注：目标靶机检测的模板需要在扫描策略里包含，若不包含，即使离线结果有数据，导入后也无法解析

离线安全基线检查过程:

(1)选择离线任务后，输入任务名称，选择核查规范

(2)导入离线结果，离线结果支持 xml 或 zip 格式导入，最后选择所需要的告警模板

4.5 脆弱性资产

WEBUI：主界面 -> 脆弱性检测-> 脆弱性资产

管理员可以对所有资产设备进行风险资产管理，在进行资产风险管理时，首先需要创建资产。通过资产，管理员可以浏览网内全部资产的数量以及资产的安全情况。资产管理界面如图 5.5-1 所示：

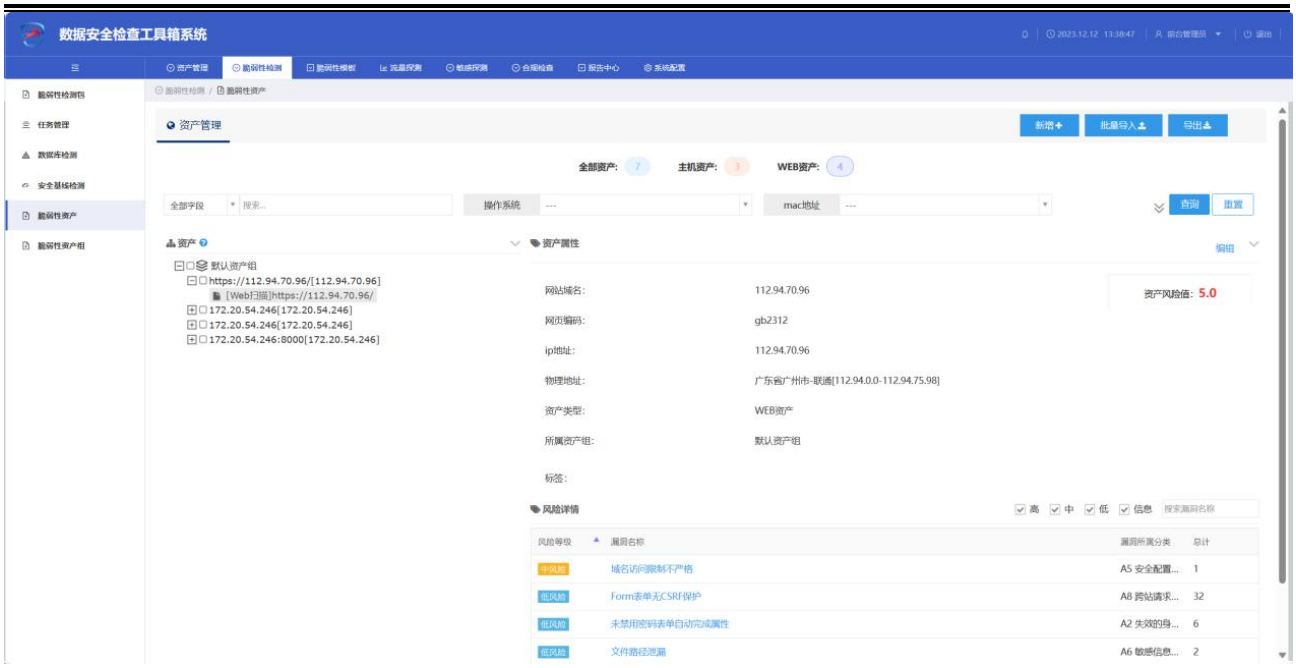


图 4.5-1 资产管理

对于其中一个资产，点击可以显示资产树，资产树由资产组、主机节点、主机以及主机上的 web 资产组成，管理员可以通过查看资产树来了解自己的网络资产情况，也可以在搜索框中按照不同维度条件搜索资产。

4.5.1 系统资产

系统资产：展开资产树中的资产组，资产组下为资产名称，资产下为该资产的扫描任务，系统资产下有系统扫描，数据库扫描，基线扫描，仅存活，口令猜解几种任务.如图 4.5.1-1

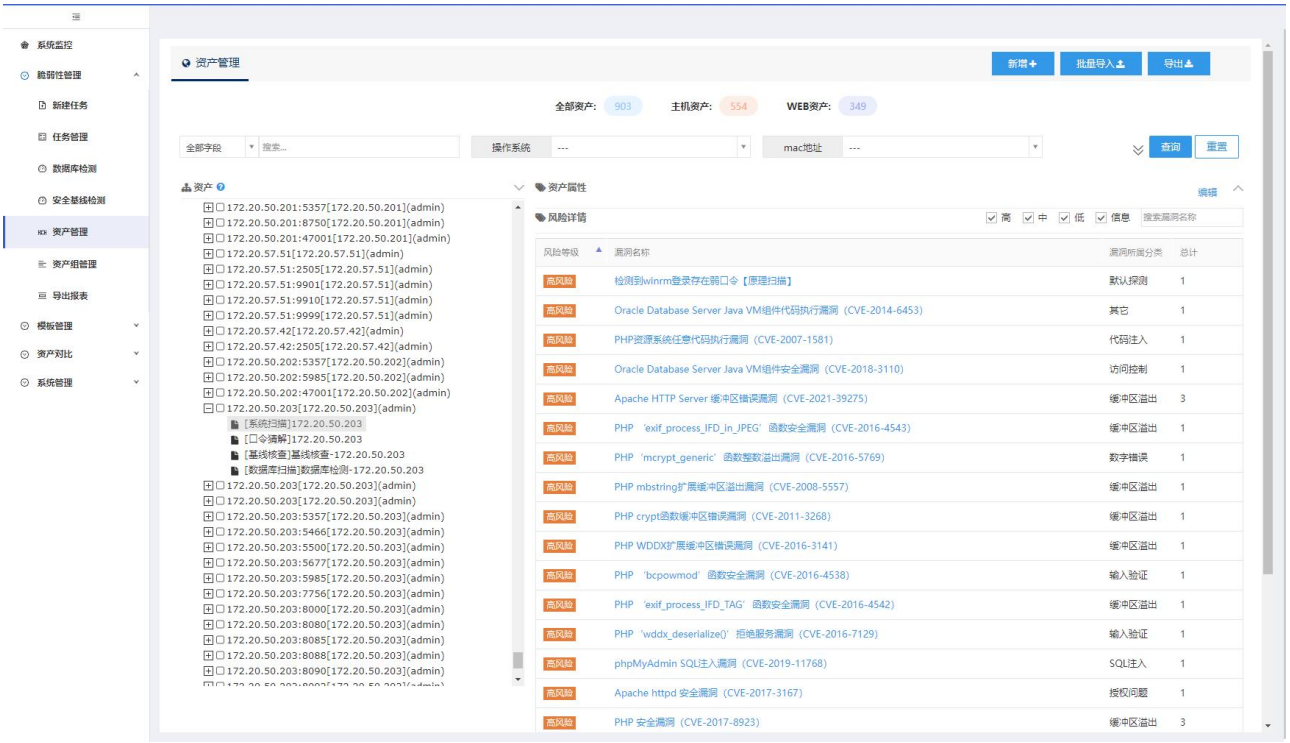


图 4.5.1-1 资产管理

➢风险详情

展示了所选资产最后一次检测时间段的检测结果

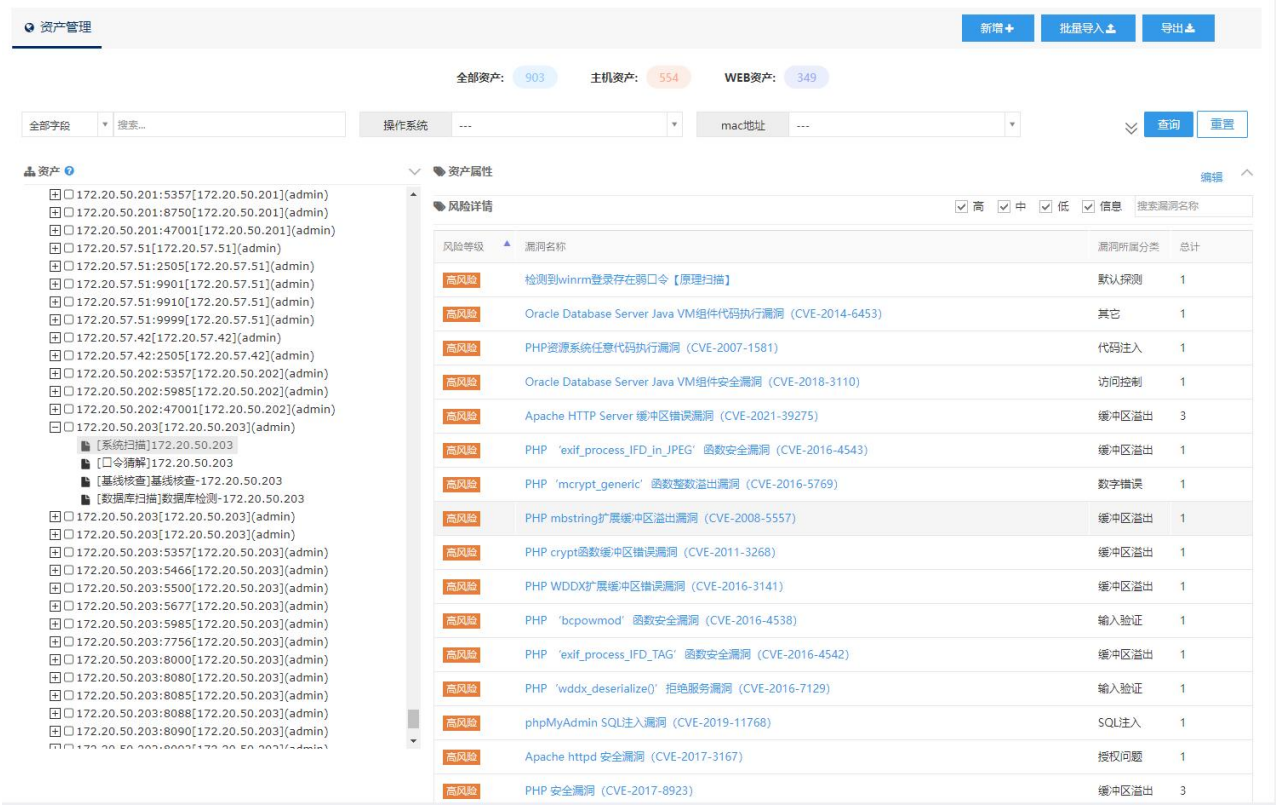


图 4.5.1-2 系统扫描--风险详情

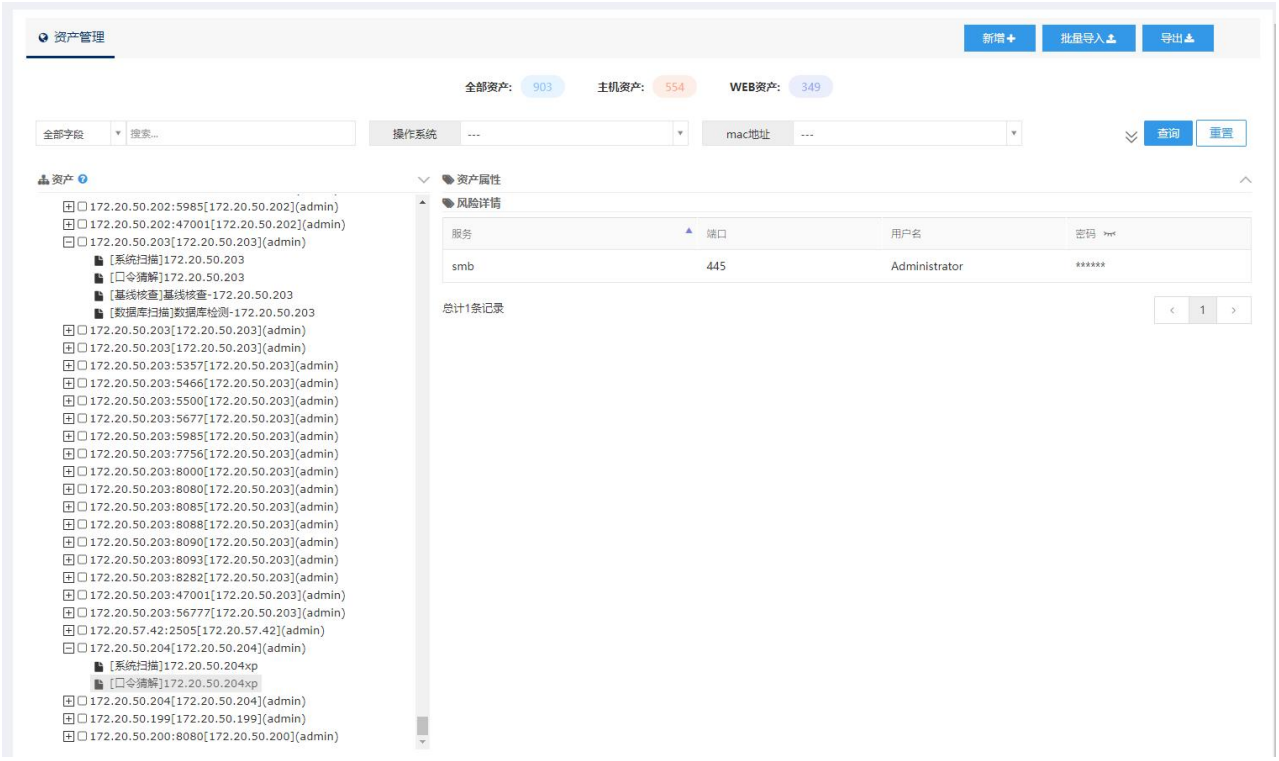


图 4.5.1-3 口令猜解--风险详情

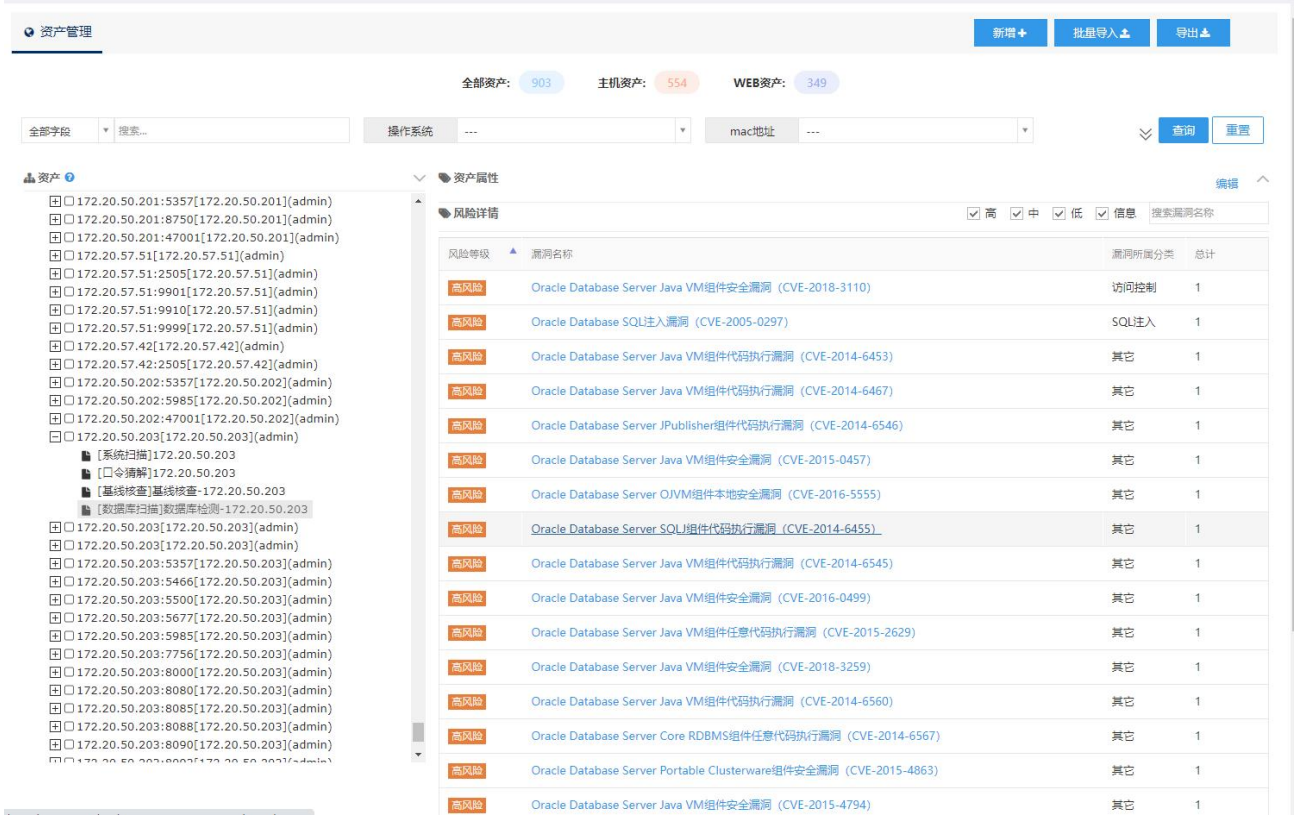


图 4.5.1-4 数据库扫描--风险详情

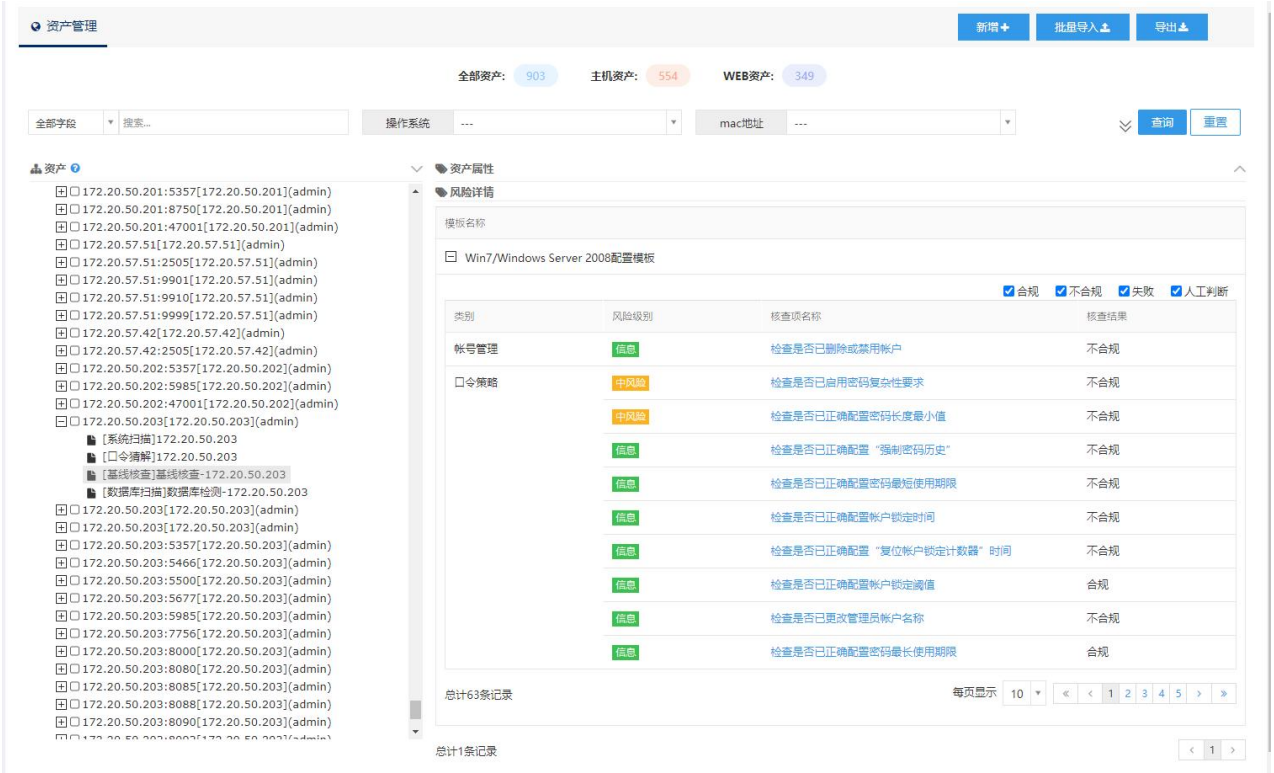


图 4.5.1-5 基线核查--风险详情

操作：点击【漏洞名称】可查看漏洞详情，即漏洞描述、解决办法、扫描详情、漏洞状态等

➢资产属性

展示了所选资产最后一次扫描的主机信息，包括该资产的主机地址、主机名称、操作系

统、物理地址以及主机资产评分等信息，如图 4.5-2 所示：

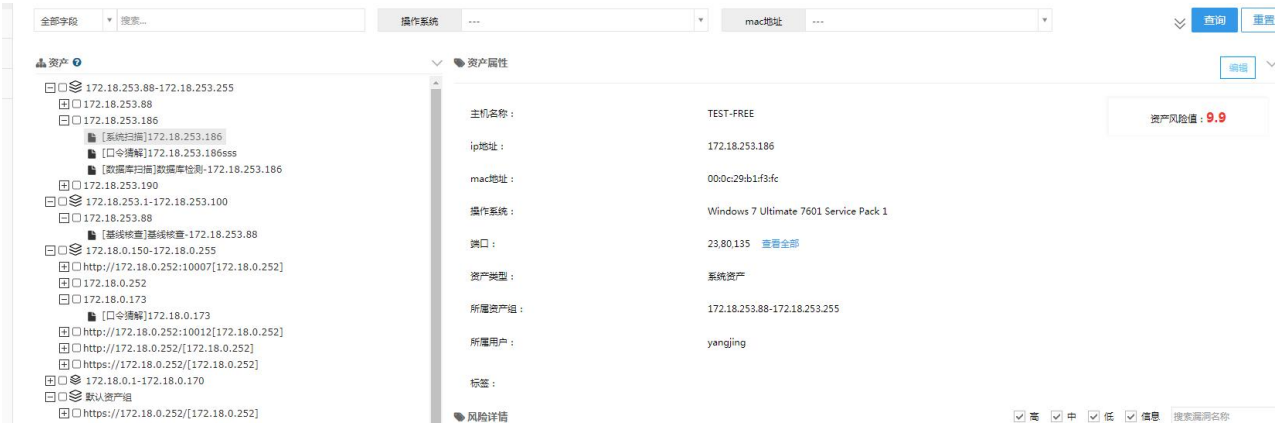


图 4.5-2 系统资产管理-资产指纹信息

操作：点击端口的【查看全部】，可弹窗展示主机上开放的所有端口

操作：点击弱口令的【查看全部】，可弹窗展示主机上检测出的弱口令和密码

4.5.2 Web 资产

Web 资产：展开资产树中的资产组，选择 web 资产，web 资产下为 web 扫描任务

➢Web 风险详情

展示了最近一次扫描结果中的所有漏洞相信信息，包括某一漏洞的风险级别、插件名称、插件所属分类以及总数，如图 5.5.2-1 所示：

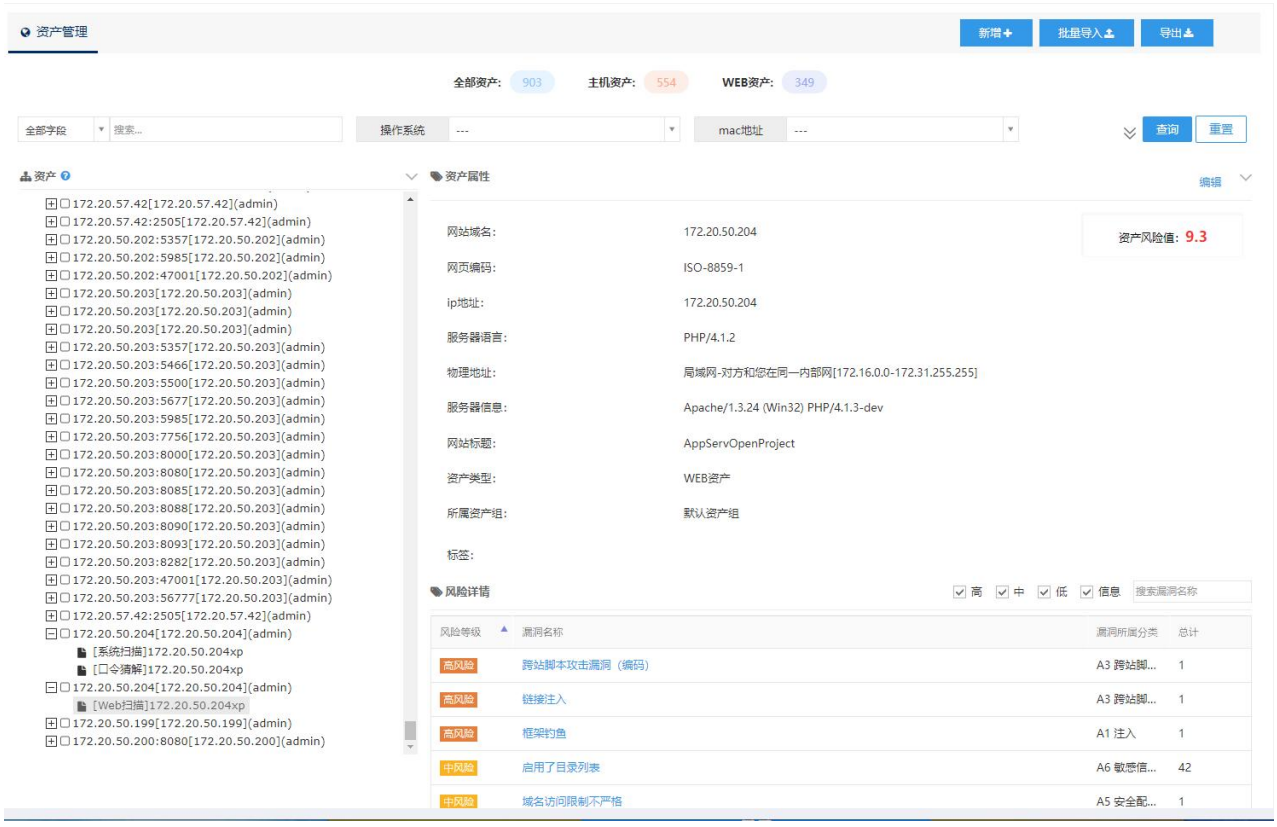


图 4.5.2-1 Web 资产管理-漏洞详情

操作：点击【漏洞名称】可查看漏洞详情，即漏洞描述、解决办法、扫描详情、漏洞状态等

➢资产属性信息

展示了每个 web 资产的主机信息，包括该资产的网站域名、IP 地址、服务器信息、网站标题、网站编码、物理地址等指纹信息，如图 4.5.2-2 所示：

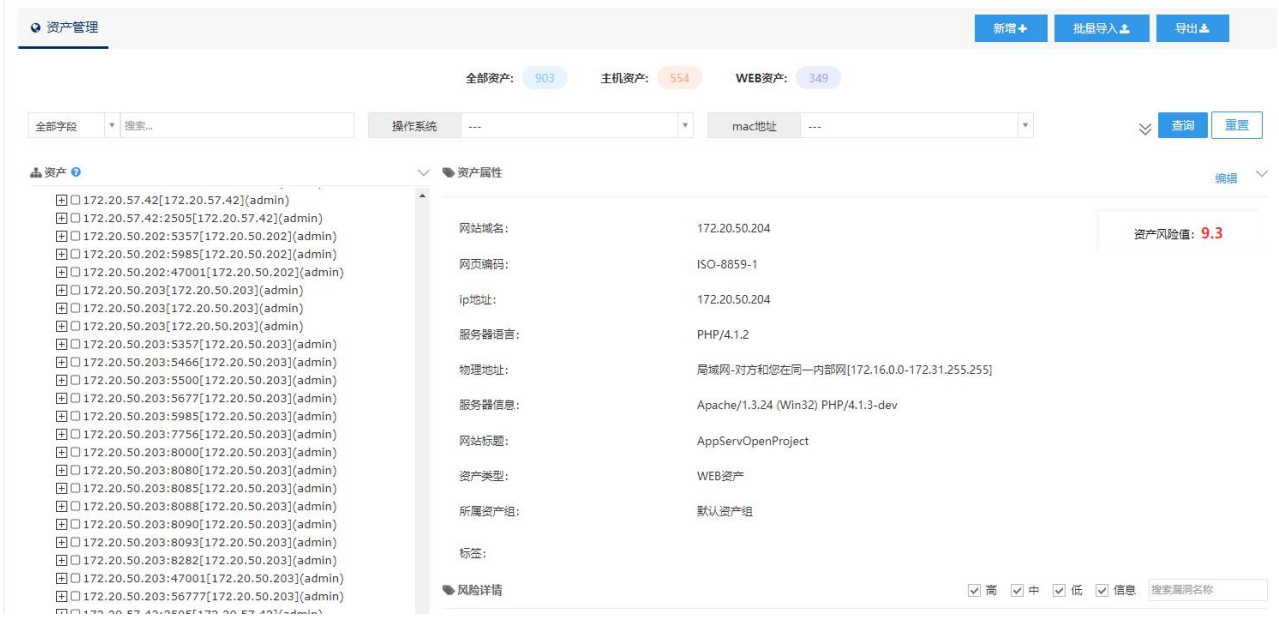


图 4.5.2-2 Web 资产管理-资产属性信息

4.5.3 新增资产

➢**手动新增资产**

点击【新增资产】按钮，在弹出的对话框中输入资产目标，完成后点击【提交】按钮即可。具体详情如图 4.5.3-1 所示：

图 4.5.3-1 Web 资产管理-新建资产

备注：资产目标支持单个、多个目标的输入，也支持 ip、url、域名多种目标格式的输入，多个资产逗号分隔

➢**批量导入资产**

点击批量导入->下载模板文件->将提前准备好的资产复制到模板文件中->上传文件-》选择所属资产组，自定义是否要添加标签-》上传,如图 4.5.3-2

图 4.5.3-2 Web 资产管理-新建资产

➢**资产添加/删除标签**

可选择多个或者单个资产对其添加标签进行分类，添加标签操作如下：

1)手动新增资产时，直接添加标签->提交即可

2)历史任务自动生成的资产->点击编辑，添加标签后提交即可

4.5.4 删除资产

用户可以对资产进行删除，可删除整个资产组。具体详细信息如图 4.5.4-1：

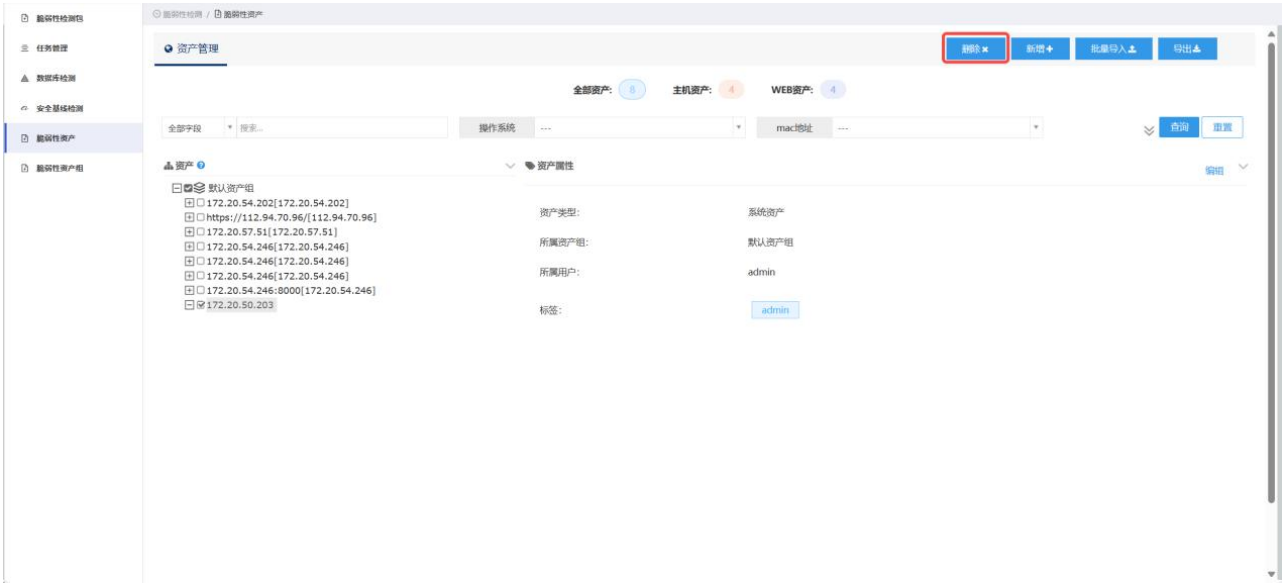


图 4.5.4-1 Web 资产管理-删除资产

4.5.5 编辑资产

可以选择单个资产编辑所选资产的资产属性，也可选择多个资产、多个节点、多个资产组进行批量编辑，对资产进行分组和添加标签

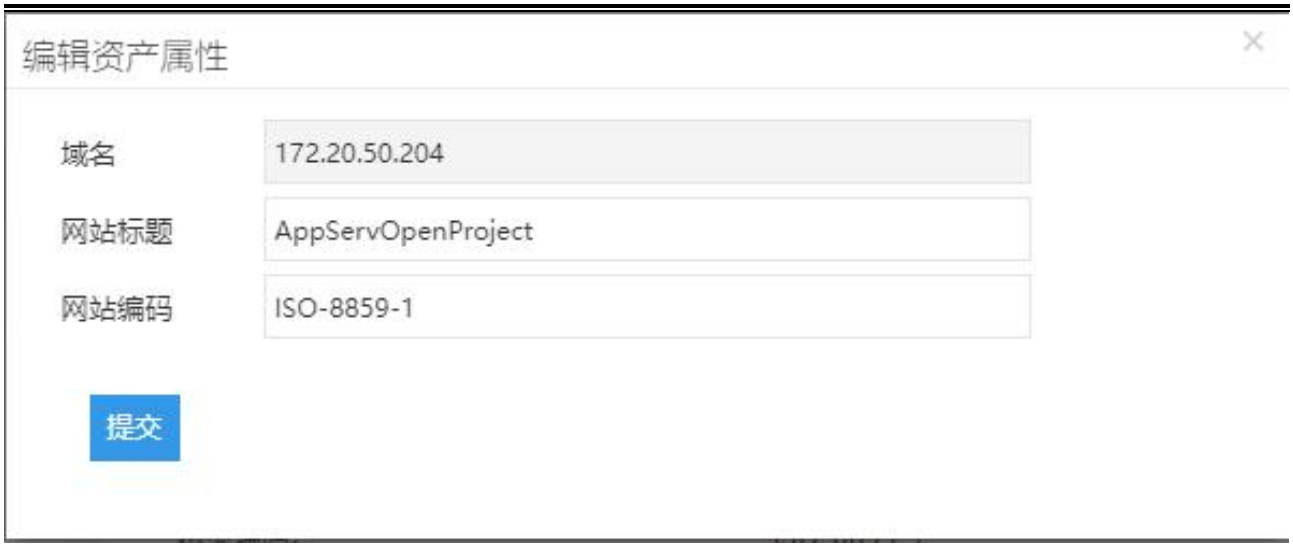


图 4.5.5-1 编辑 web 资产属性

图 4.5.5-1 编辑系统资产属性

4.5.6 查询资产

支持多个维度的条件搜索，具体搜索操作如下：

1)进入资产管理界面->点击，展开所有搜索条件，如下

图 4.5.6-1 资产搜索条件

2) 配置不同查询参数->点击查询，查看符合条件的资产信息

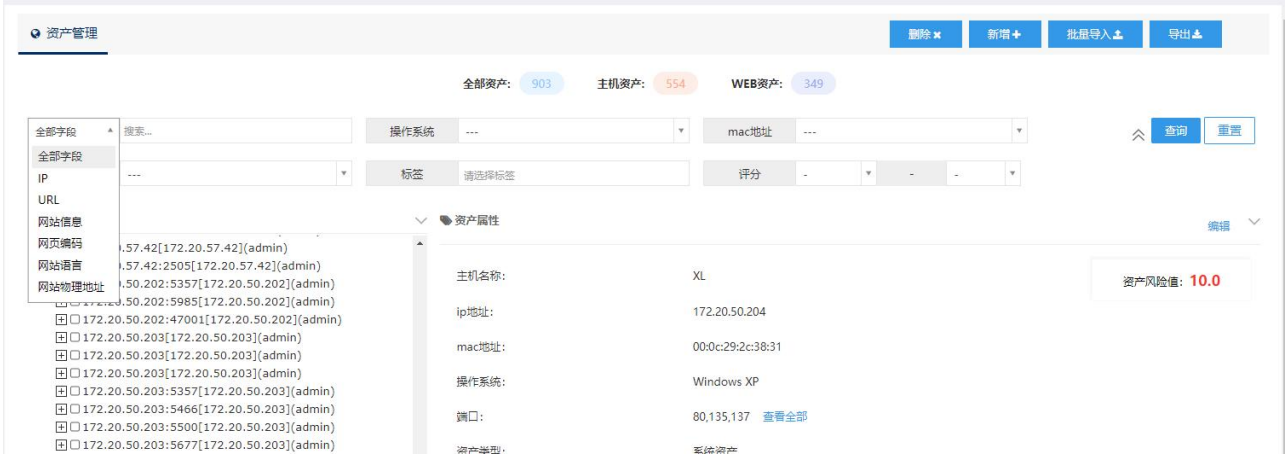


图 4.5.6-2 资产搜索

查询条件参数说明：如下表

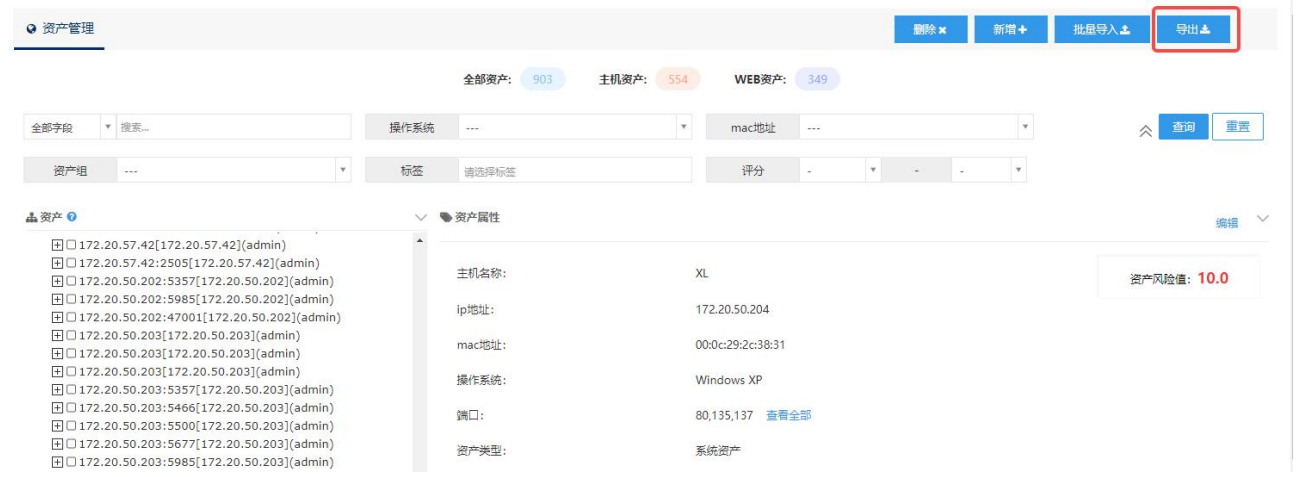
表 4.5.6-1 搜索条件参数说明

参数	描述
资产名称	主机资产或者 web 资产名称
资产 ip	主机资产的 ip
资产 url	Web 资产的 url
服务器信息	Web 资产使用的服务器信息
网页编码	Web 资产使用的网页编码技术
服务器语言	Web 资产使用的服务器语音
物理地址	资产设备所在的物理地址
操作系统	主机设备的操作系统类型
Mac 地址	主机设备的 mac 地址
资产组	资产所属的资产组，下发任务时指定或者新增资产时指定
标签	资产标签，由用户定义
评分	资产经过扫描后的系统给出的风险值，风险值越高说明资产越不安全

3)单击【重置】按钮，可以清空查询条件，重新查询资产信息。

4.5.7 资产导出

在资产管理界面->选择资产或者不选择->点击导出按钮，如下：可将系统上所选资产或者全部资产导出到 excel



	A	B
1	资产组名称	资产
2	192.168.5.1	192.168.5.1[192.168.5.1]
3		192.168.5.1[192.168.5.1]
4	新增测试组	172.20.50.199[172.20.50.199]
5		172.20.50.199[172.20.50.199]
6	test	
7	默认资产组	172.20.52.115
8		
9		
10		

图 4.5.7-1 资产导出

4.6 脆弱性资产组

WEBUI：主界面 -> 脆弱性检测->脆弱性资产组

资产组管理模块 dcbox 用户具有该功能模块的操作权限。都可对该模块功能进行操作管理。dcbox 用户可以对所有用户的资产组进行操作，普通用户只能查看并操作自己的资产组。用户可以根据自身资产系统的组织结构或者网络拓扑通过资产组对其进行分类分组

4.6.1 新增资产组

操作：在脆弱性资产组页面->点击【新增】->输入资产组名称->点击提交

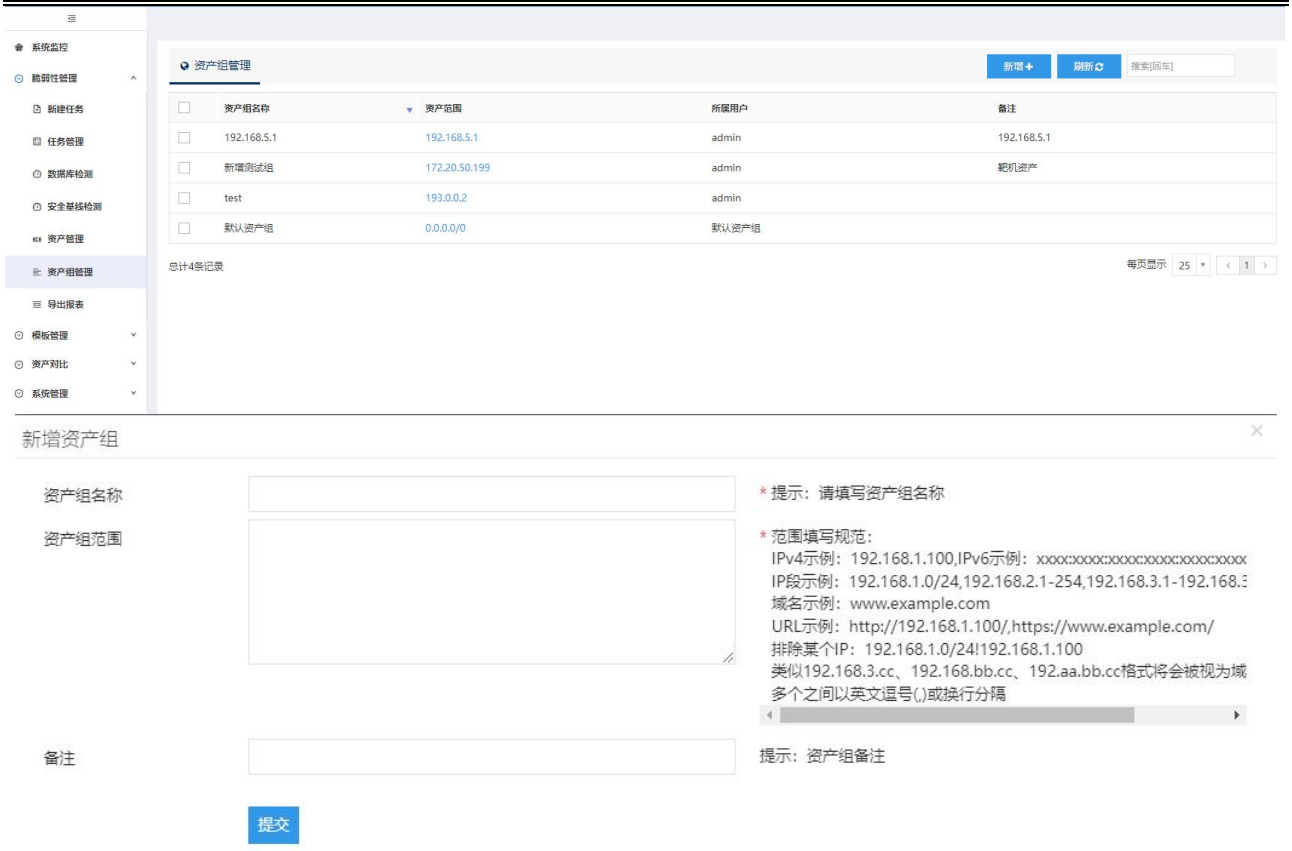


图 4.6.1-1 新增资产组

编辑资产组同理：选择已有的资产组->点击【编辑】->修改资产组名称后提交即可修改

4.6.2 删除资产组

资产组删除包含了 2 种情况：资产组下无资产、资产组下有资产，当资产组下有资产时，删除资产组该资产组下的资产全部划分到默认资产组下，资产管理和资产资产组管理都没有该资产组。

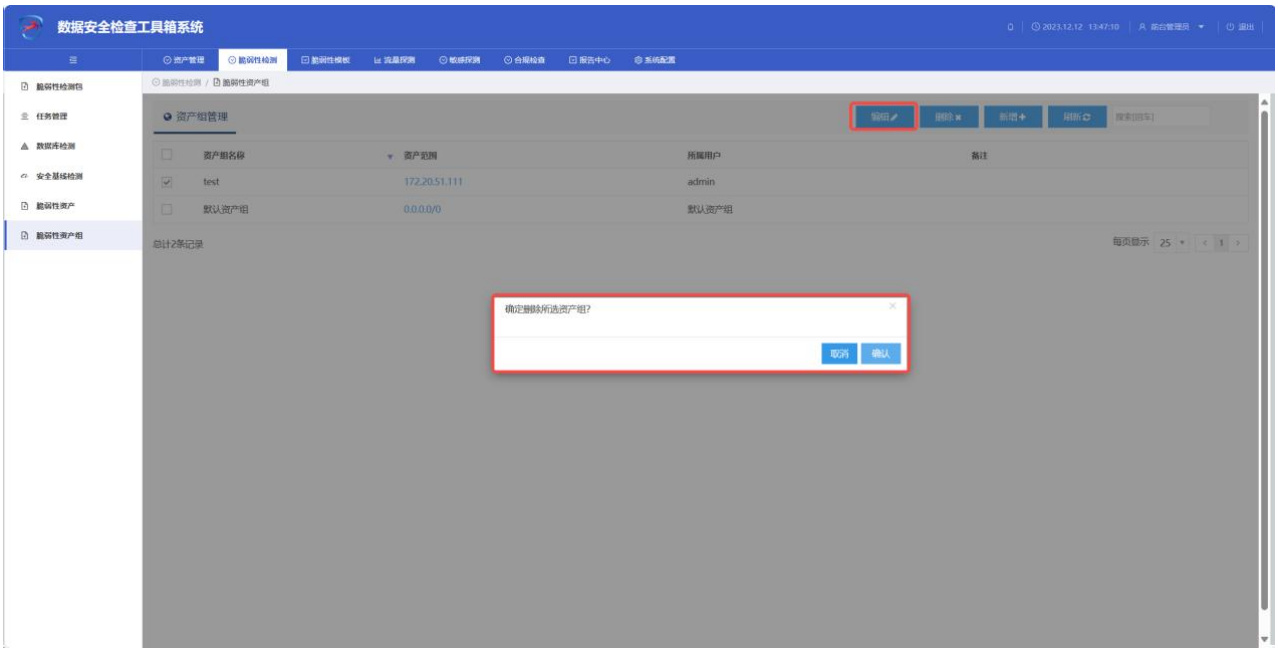


图 4.6.2-1 删除资产组

4.6.3 新建基线策略

点击【增加策略】，填写相应的基线策略名称，点击【保存】按钮即可新建成功。新增的基线策略默认包含所有插件，可通过“启用”“禁用”来进行插件的选择。如图 4.6.3 所示

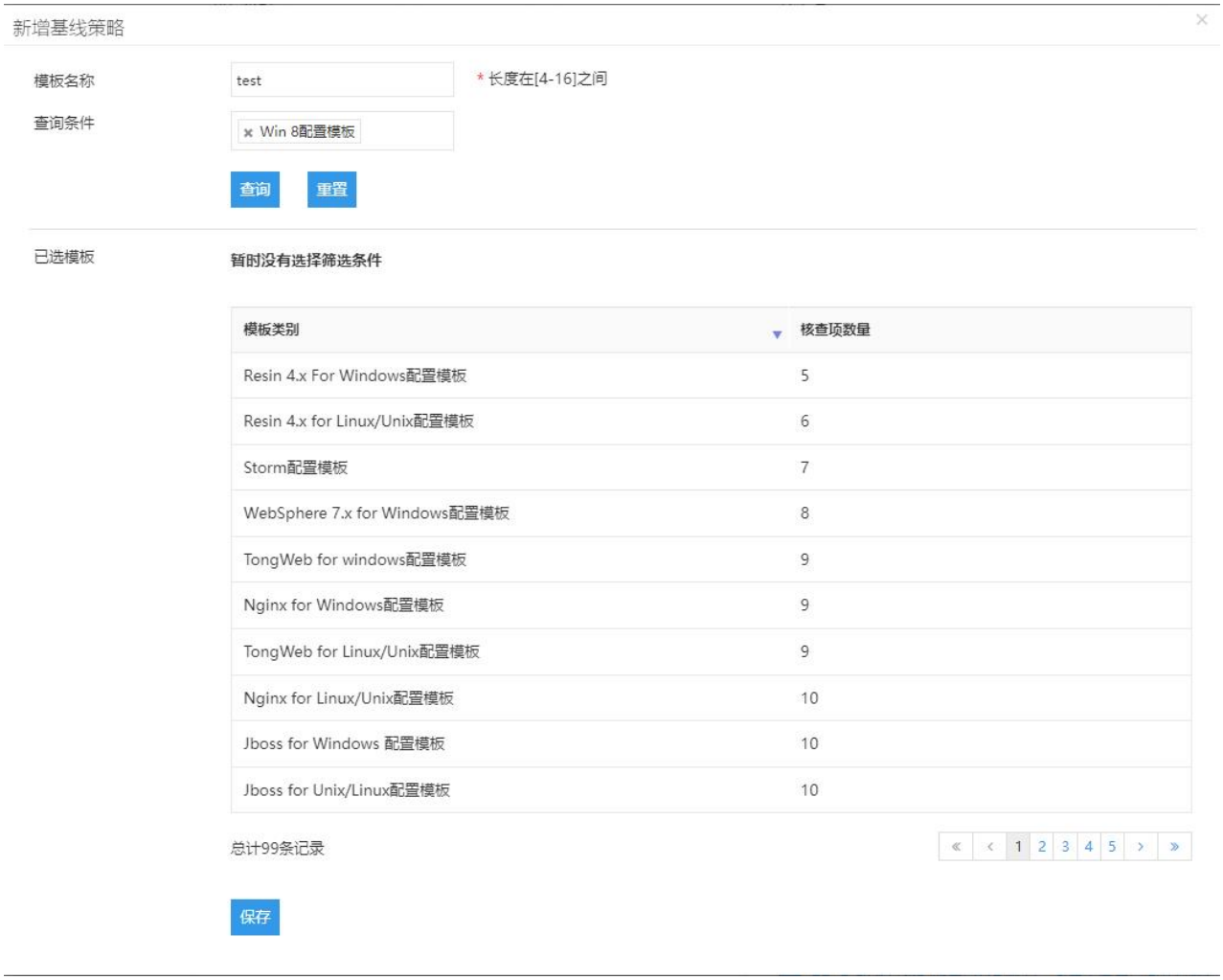


图 4.6.3 新建基线策略

4.6.4 基线离线模板

基线离线模板可以提供用户下载，远程对主机进行扫描生成离线结果

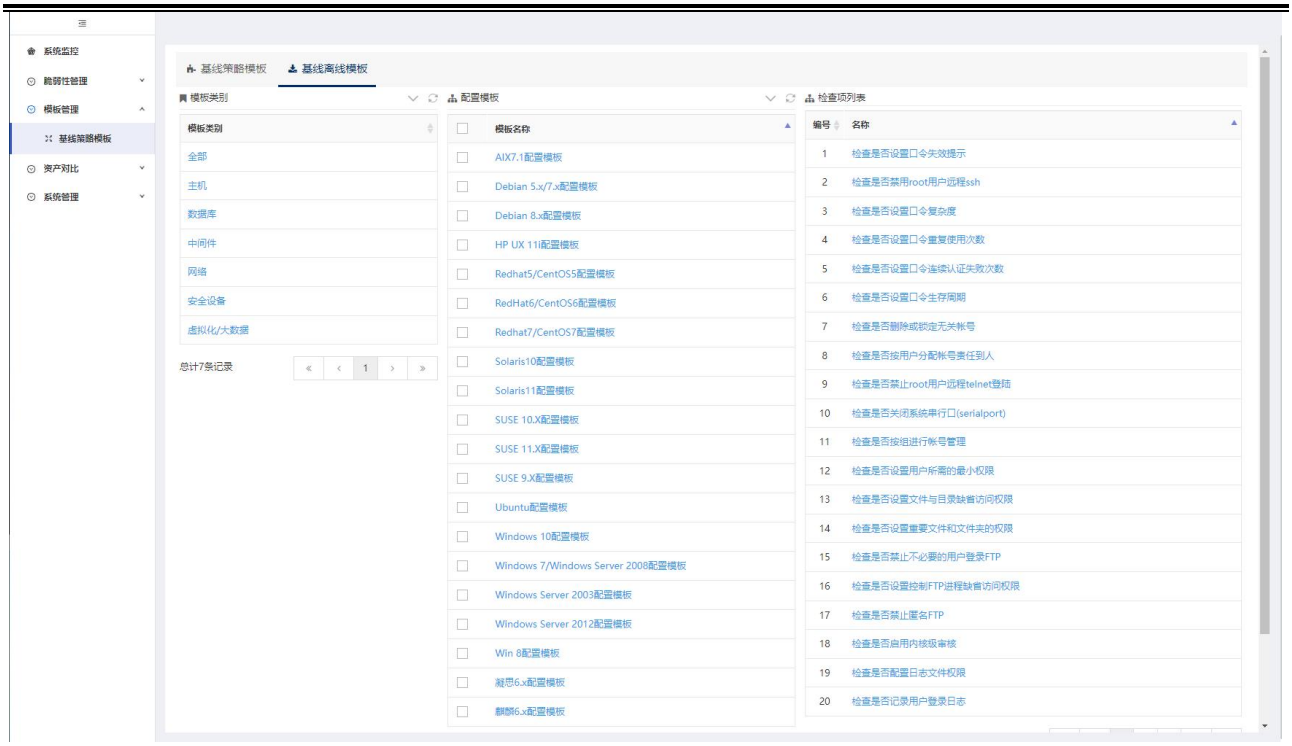

系统监控
脆弱性管理
模板管理
基线策略模板
资产对比
系统管理
基线策略模板
基线离线模板
模板类别
配置模板
检查项列表
模板类别
全部
主机
数据库
中间件
网络
安全设备
虚拟化/大数据
总计7条记录
模板名称
AIX7.1配置模板
Debian 5.x/7.x配置模板
Debian 8.x配置模板
HP UX 11i配置模板
Redhat5/CentOS5配置模板
RedHat6/CentOS6配置模板
Redhat7/CentOS7配置模板
Solaris10配置模板
Solaris11配置模板
SUSE 10.X配置模板
SUSE 11.X配置模板
SUSE 9.X配置模板
Ubuntu配置模板
Windows 10配置模板
Windows 7/Windows Server 2008配置模板
Windows Server 2003配置模板
Windows Server 2012配置模板
Win 8配置模板
凝思6.x配置模板
麒麟6.x配置模板
编号
名称
1 检查是否设置口令失效提示
2 检查是否禁用root用户远程ssh
3 检查是否设置口令复杂度
4 检查是否设置口令重复使用次数
5 检查是否设置口令连续认证失败次数
6 检查是否设置口令生存周期
7 检查是否删除或锁定无关帐号
8 检查是否按用户分配帐号责任到人
9 检查是否禁止root用户远程telnet登陆
10 检查是否关闭系统串行口(serialport)
11 检查是否按组进行帐号管理
12 检查是否设置用户所需的最小权限
13 检查是否设置文件与目录缺省访问权限
14 检查是否设置重要文件和文件夹的权限
15 检查是否禁止不必要的用户登录FTP
16 检查是否设置控制FTP进程缺省访问权限
17 检查是否禁止匿名FTP
18 检查是否启用内核级审核
19 检查是否配置日志文件权限
20 检查是否记录用户登录日志

图 4.6.4 基线模板

五. 脆弱性模板

5.1 基线策略模板

WEBUI：主界面 -> 脆弱性模板 -> 基线策略模板

安全基线核查功能主要是进行专业检查的，可以有效提高检查结果的准确性和合规性，用以在设备的上线安全检查、第三方入网安全检查、合规安全检查、日常安全检查和安全服务任务工作中。

预置的基线策略规则插件，可灵活自定义所需策略规则。具体的详情如下图 5.1 所示：

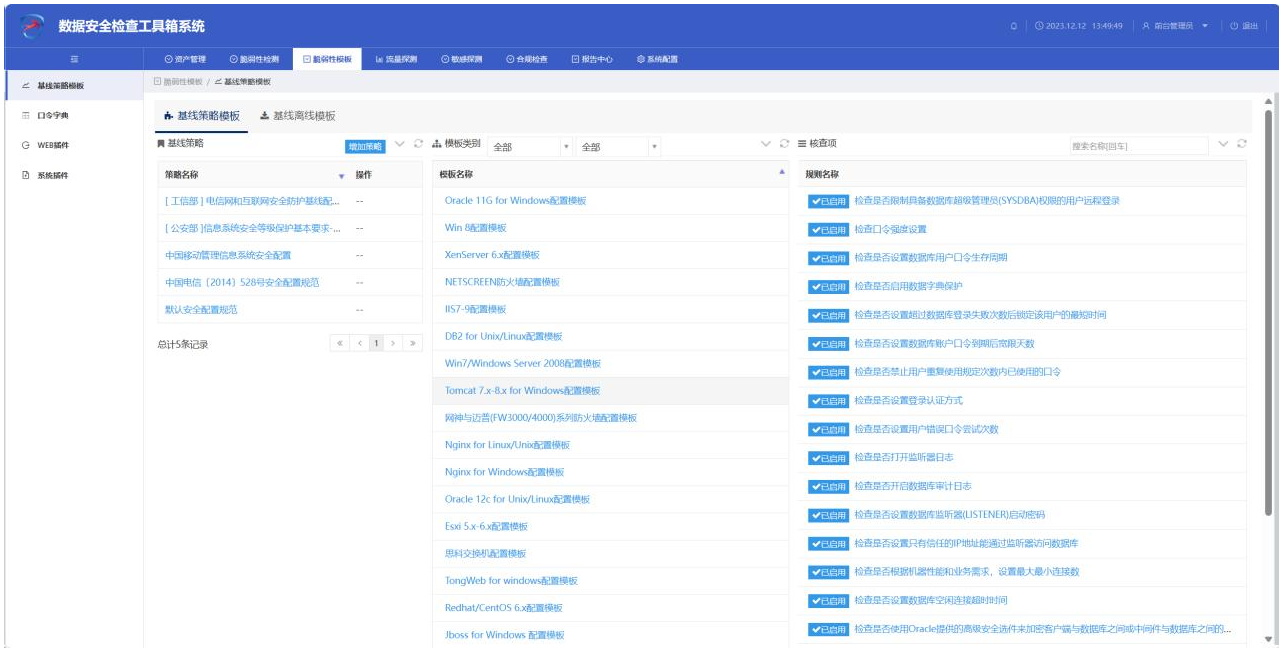


图 5.1 基线策略模板

5.1.1 新建基线策略

点击【增加策略】，填写相应的基线策略名称，点击【保存】按钮即可新建成功。新增的基线策略默认包含所有插件，可通过“启用”“禁用”来进行插件的选择。如图 5.1.1 所示

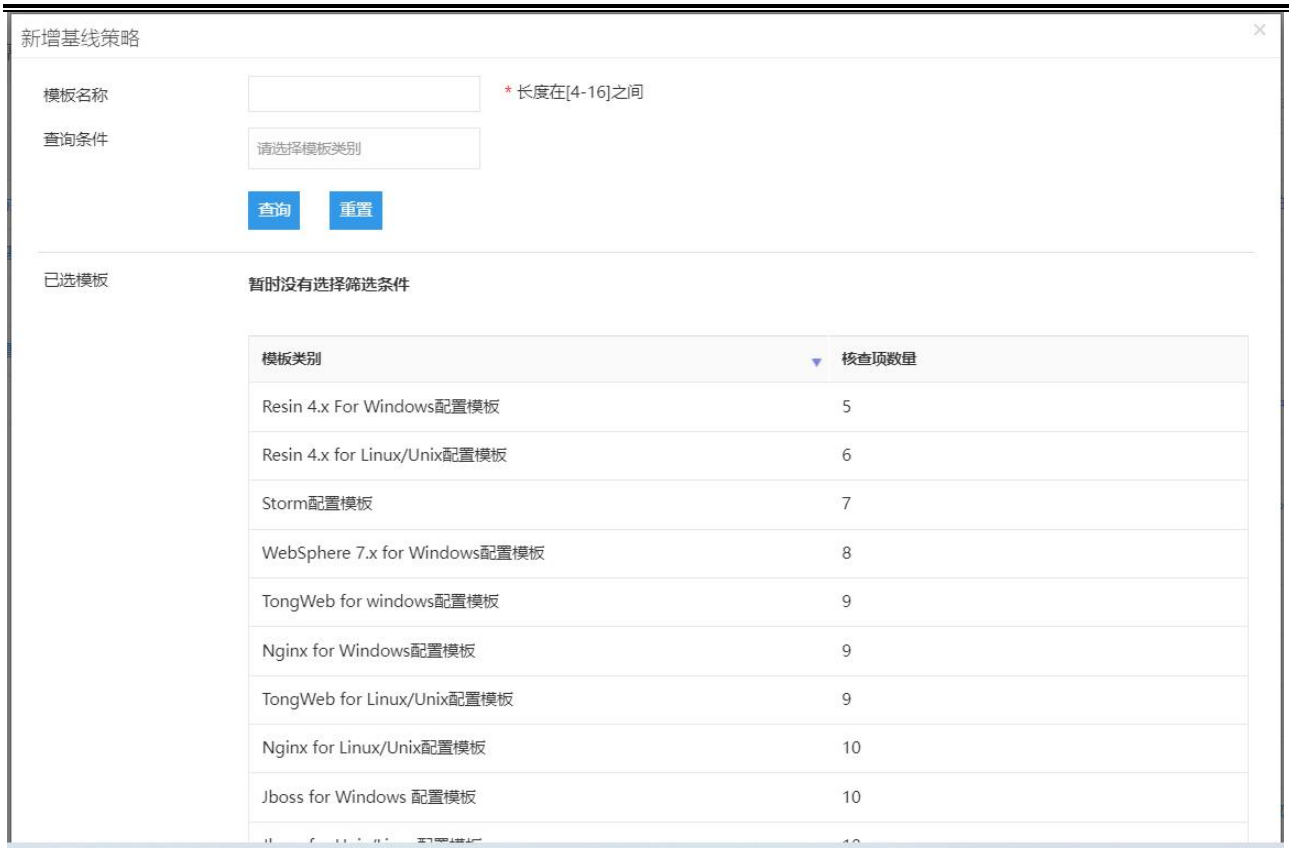


图 5.1.1 新建基线策略

5.1.2 基线离线模板

基线离线模板可以提供用户下载，远程对主机进行扫描生成离线结果

离线任务：将在目标靶机上执行的基线核查结果导入到系统，直接进行解析和结果查看，没有远程登录和检测的过程

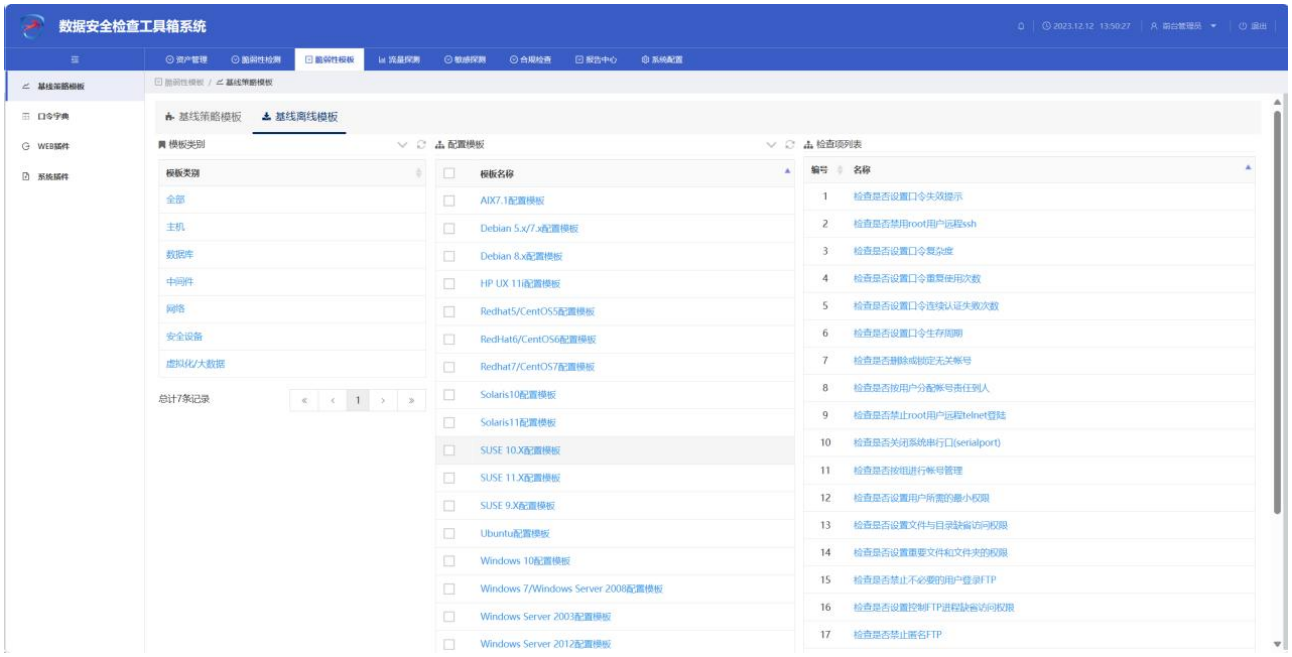


图 5.1.2-1 基线模板

离线安全基线检查过程:

(1)选择离线任务后，输入任务名称，选择核查规范

(2)导入离线结果，离线结果支持 xml 或 zip 格式导入，最后选择所需要的告警模板

5.2 口令字典

WEBUI：主界面 -> 脆弱性模板 -> 口令字典

系统默认的有三种字典：组合字典，用户名字典，密码字典。组合字典中用户名和密码都有，主要是针对弱口令扫描时用户名和密码同时匹配才定义为弱口令。用户名字典和密码字典主要是弱口令扫描选择标准模式时对用户名和密码分开单独进行匹配。具体如图 6.2 所示：

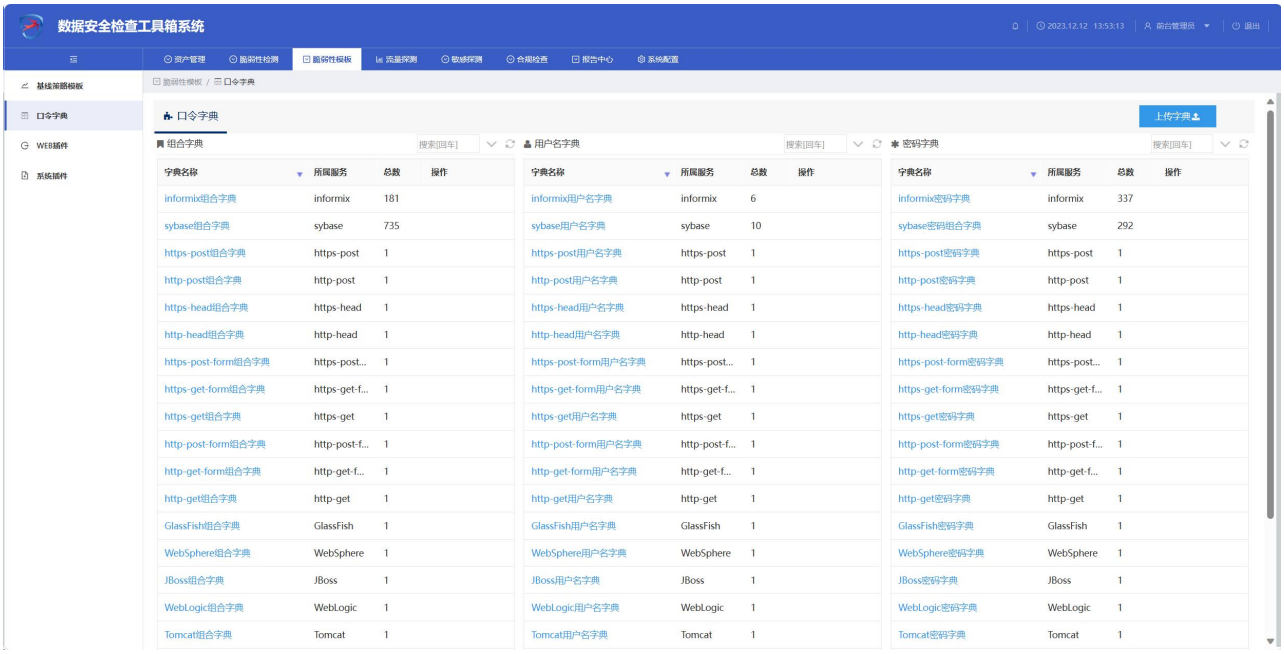


图 5.2 口令字典

5.2.1 上传口令字典

用户可以自己上传弱口令字典，字典格式既可以为组合模式，也可以为标准模式，类型统一为 dic 格式，不支持其他类型的字典，上传的文件大小正常不超过 10MB。具体如下图 6.2.1-1 所示：

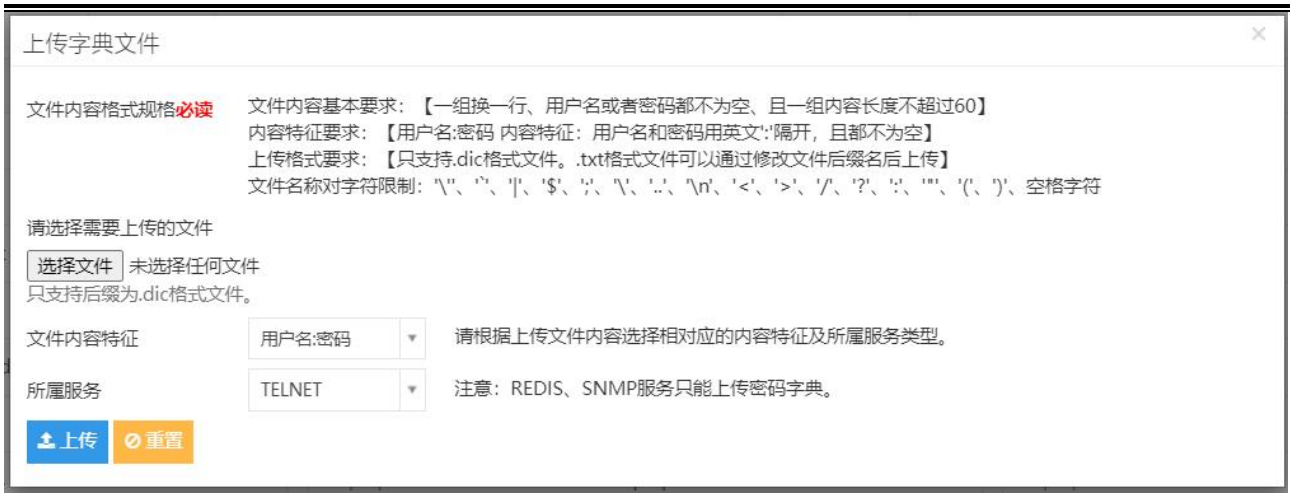


图 5.2.1-1 选择口令字典文件

选择要上传的弱口令字典文件，相应的文件内容特征，以及所属服务，点击【提交】即可上传成功。上传成功后界面如下图 5.2.1-2 所示：

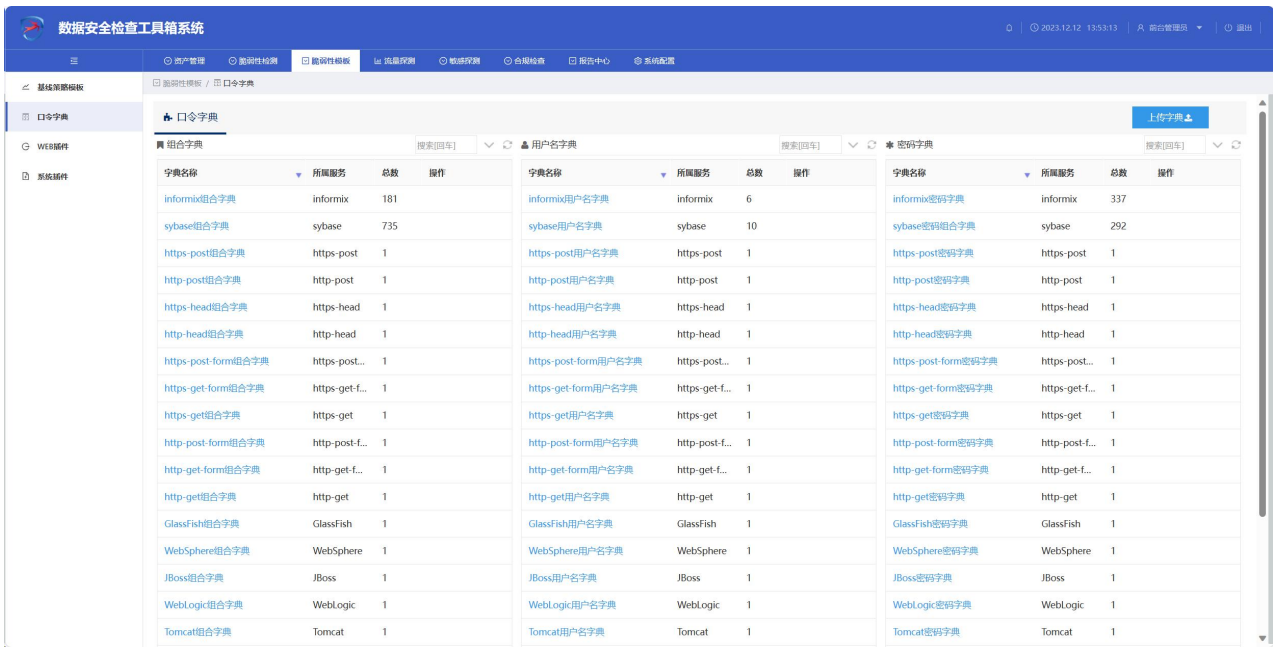


图 6.2.1-2 上传口令字典

5.3 WEB 插件

WEBUI：主界面 -> 脆弱性模板 -> WEB 插件

预置的 Web 漏洞插件库，包含当前最新的检测规则，提供全面的安全扫描策略，并能灵活定义扫描策略。如图 5.3 所示：

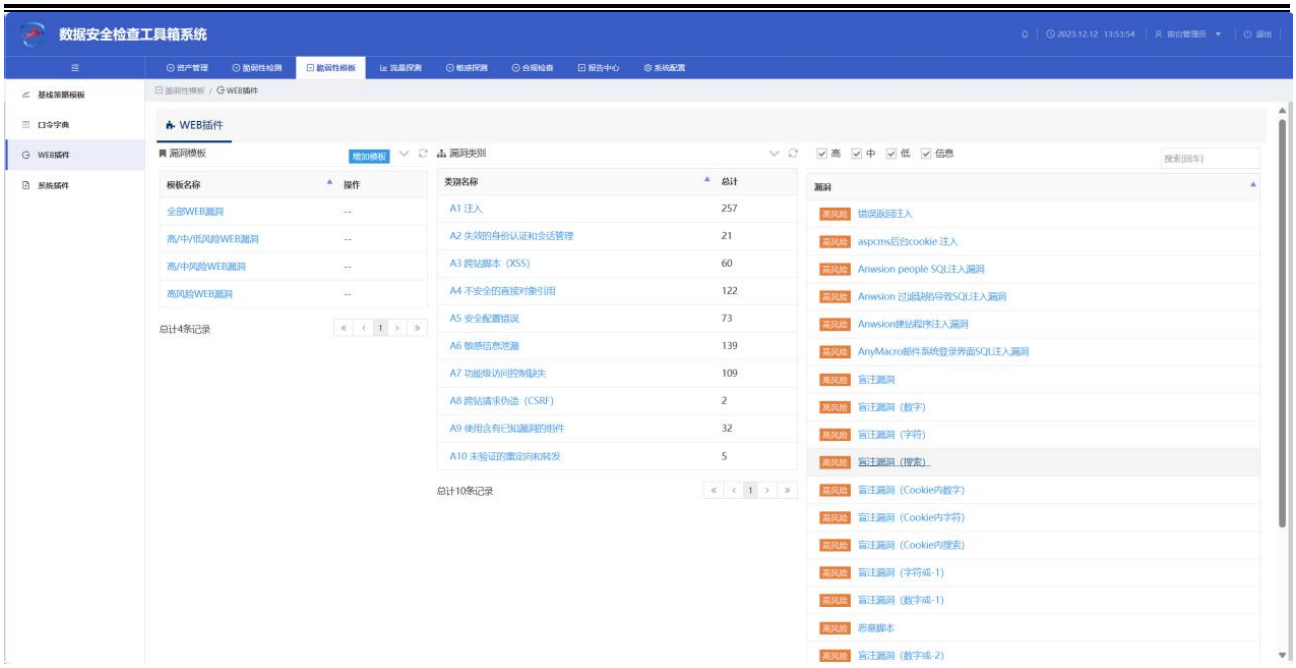


图 5.3 Web 插件

5.3.1 新增 Web 插件模板

点击【增加模板】，填写相应的 Web 插件模板名称，点击【保存】按钮即可新建成功。如图 5.3.1-1 所示：

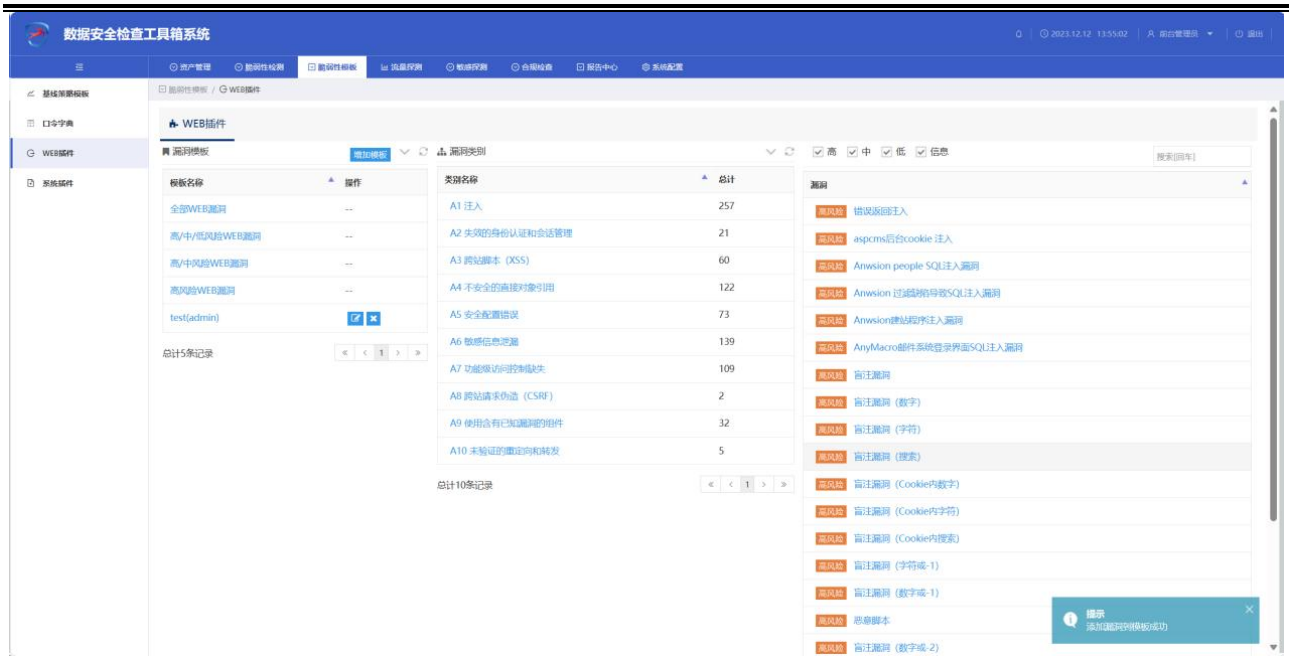


图 5.3.1-1 新增 Web 插件模板

5.4 系统插件

WEBUI：主界面 -> 策略模板 -> 系统插件

系统插件包含了所有的漏洞插件，可以对插件策略模板、漏洞类别、漏洞进行相应的排序，查询。可通过搜索框搜索某一确定的漏洞名称、漏洞编号、CVE 号。如下图 6.4 所示：

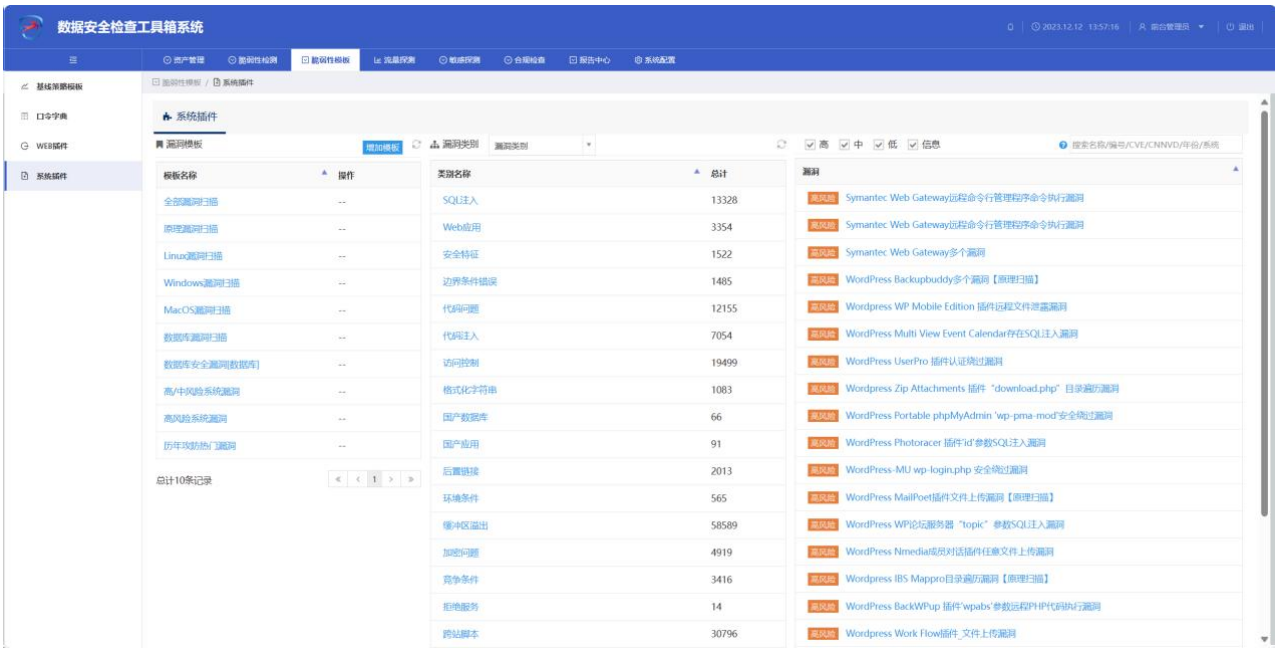
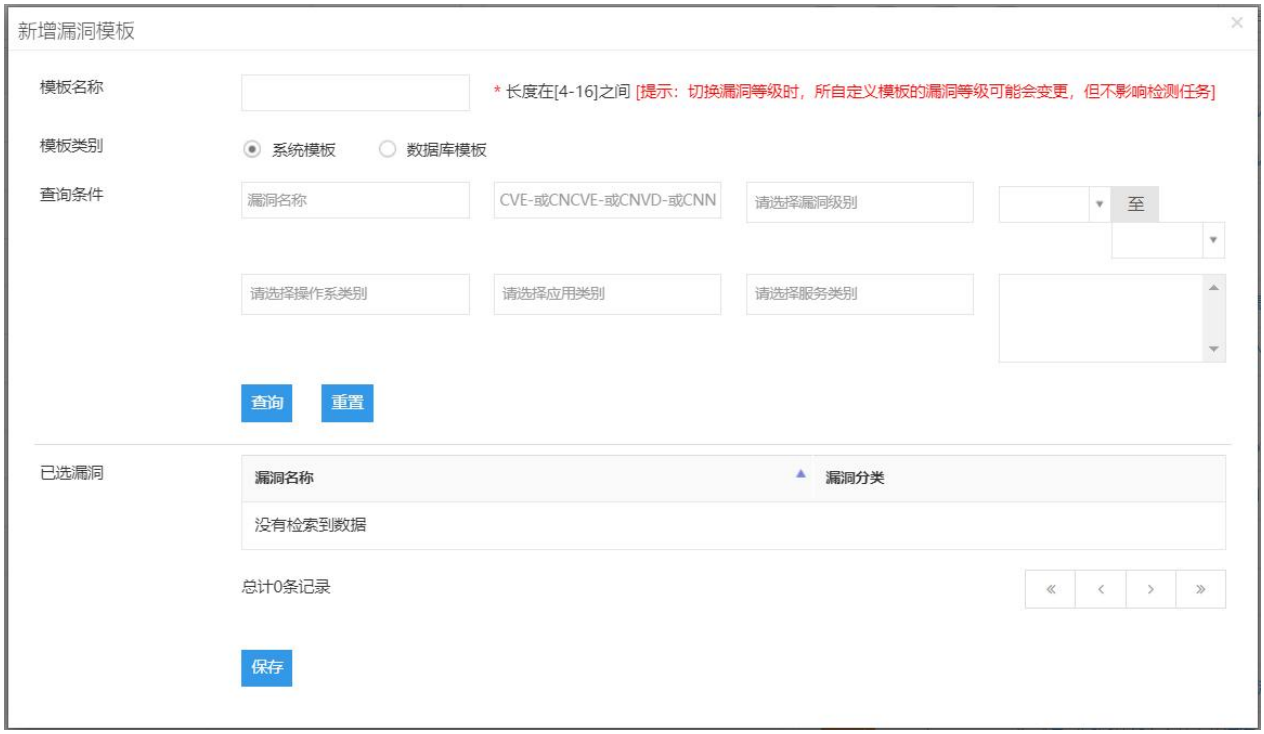


图 5.4 系统插件

5.4.1 新增系统插件模板

用户除了可以使用系统默认提供的检测库模板外，也可以自定义规则库，我们提供了规则库模板的随意组合功能，可以有选择、有针对性的制定模板，确保检测的高效性。

点击【增加模板】，编写相应的系统插件模板名称即可新建成功。如图 5.4.1-1 所示：



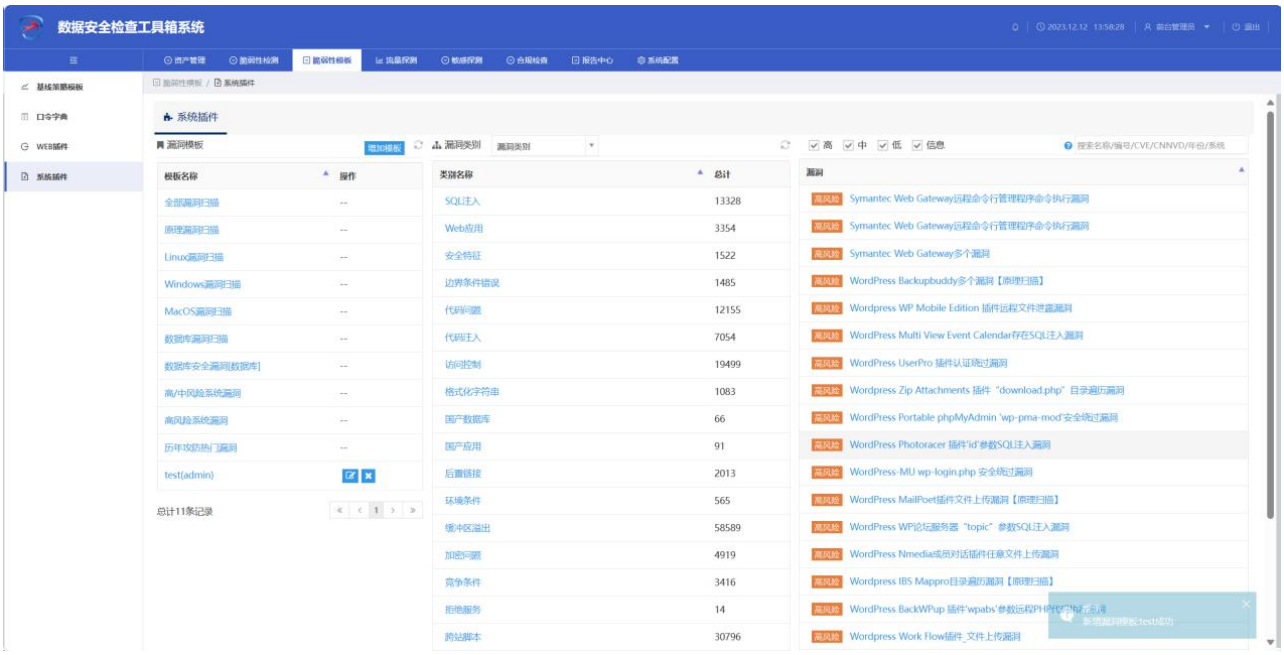


图 5.4.1-1 新增系统插件模板

⚠：自定义插件模板可以进行相应的名称编辑、插件启用、禁用等，但系统默认的插件模板不能进行编辑、删除、以及启用或禁用某一插件。

六. 流量探测

WEBUI：主界面 -> 流量探测

流量探测包括新建任务、探测预览页面，其中探测预览中包括 10 种不安全行为预览。

6.1 新建任务

WEBUI：主界面 -> 流量探测 ->新建任务

6.1.1 新建任务

流量探测页面可以根据 IP 段、探测类型、探测时间段、API 存活探测新建不同的任务，其中探测类型预计支持 API 与数据库两种，目前只支持 API 类型，API 类型中只支持 http 类型的流量探测。探测时间段可分别选中 5 分钟/10 分钟/1 小时/2 小时，API 存活探测，选是时会进行 API 存活的探测，并在 API 清单列表中新增相应的记录，选否不进行 API 存活探测。

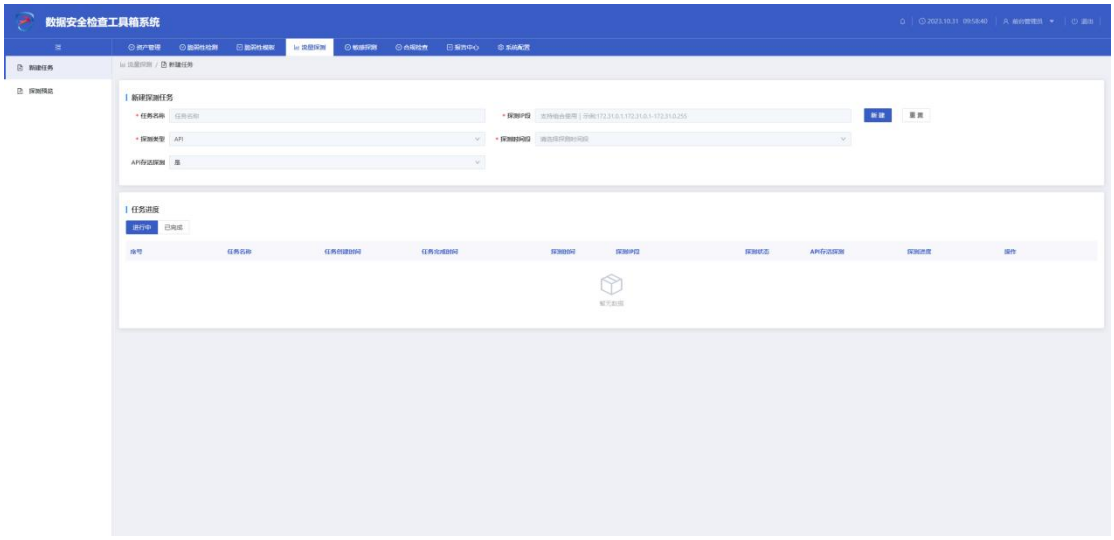


图 6.1.1 新建任务

6.2 探测预览

WEBUI：主界面 -> 流量探测 ->探测预览

6.2.1 探测预览

探测预览页面展示探测完成任务的安全情况，及所有探测任务的综合概况。安全总览展示探测次数，以及探测结果中安全与不安全事件总数。右侧不安全行为预览即 17 种不安全模型对应的事件，若触发对应事件即说明流量片段非安全。

当前模型包括：cookie 中包含密码、数据泄露风险、敏感数据导出、单次返回数据量过

大、敏感数据传输、api 参数可遍历、明文传输密码、机器访问行为、命令执行 api、访问超限、明文传输弱口令、数据库查询 api、未鉴权访问、数据出境风险、出境账实不符、持续数据泄露、账号高频访问。

任务详情展示所有已完成的探测任务，及相关参数与安全与否。不安全的任务将展示具体安全行为内容，点击“详情”即可查看。

探测预览数据保留 30 天数据。

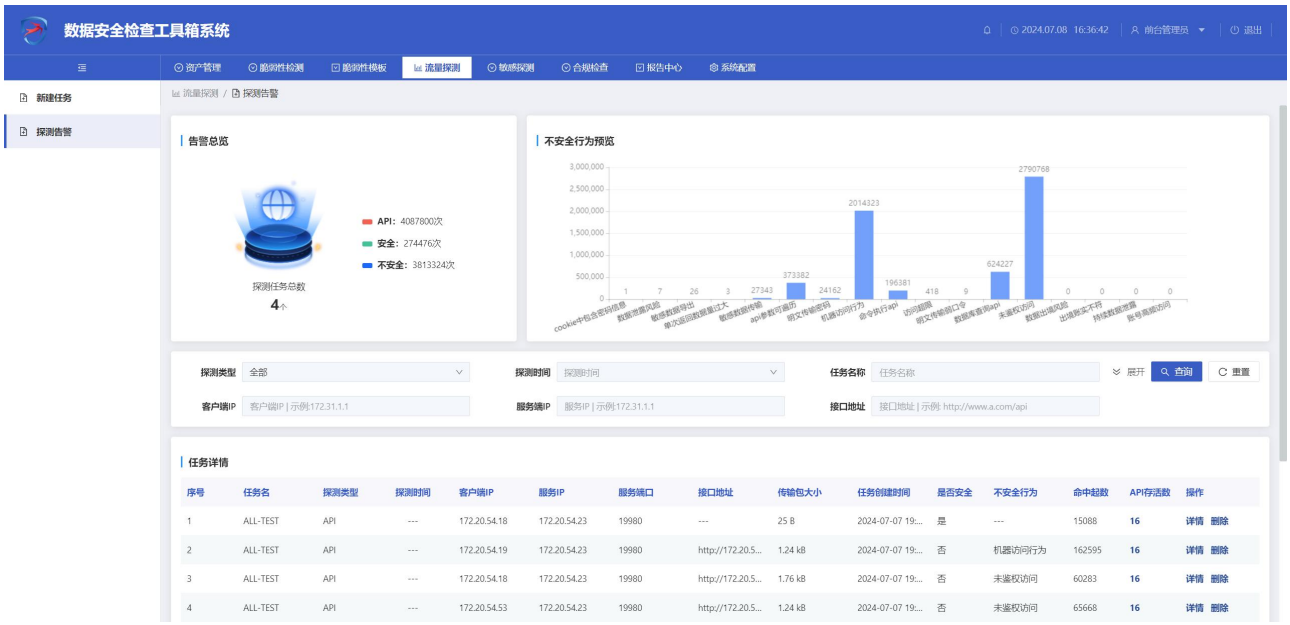


图 6.2.1 探测预览

七. 敏感探测

7.1 数据库资产

WEBUI：主界面 -> 敏感探测 -> 数据库资产

对数据库进行深度扫描，100+ 敏感字段规则风险发现数据库中的敏感字段。

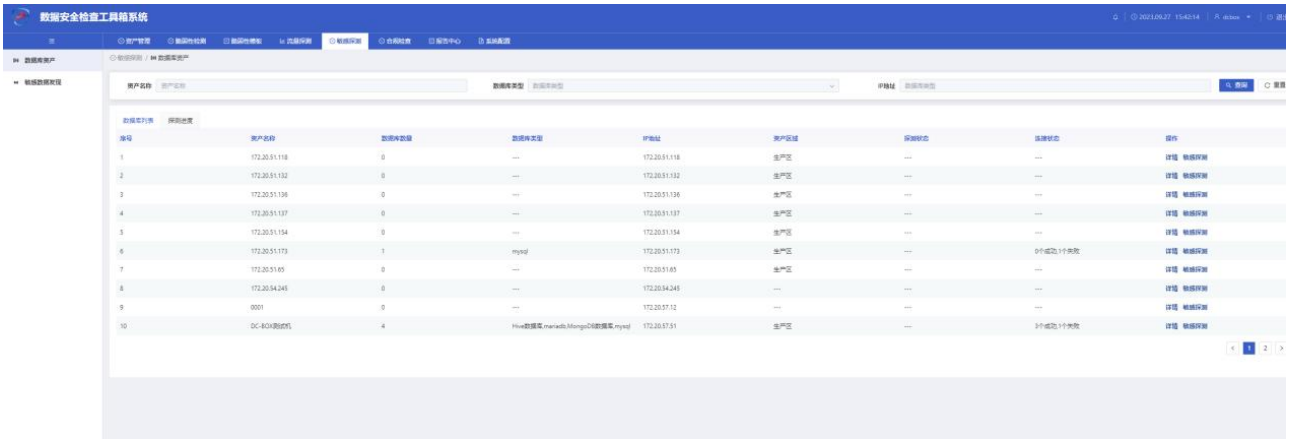


图 7.1 数据库资产

7.1.1 数据库列表

WEBUI：主界面 -> 敏感探测 -> 数据库资产-> 数据库列表

资产管理中的所有数据库资产会在表单中显示。

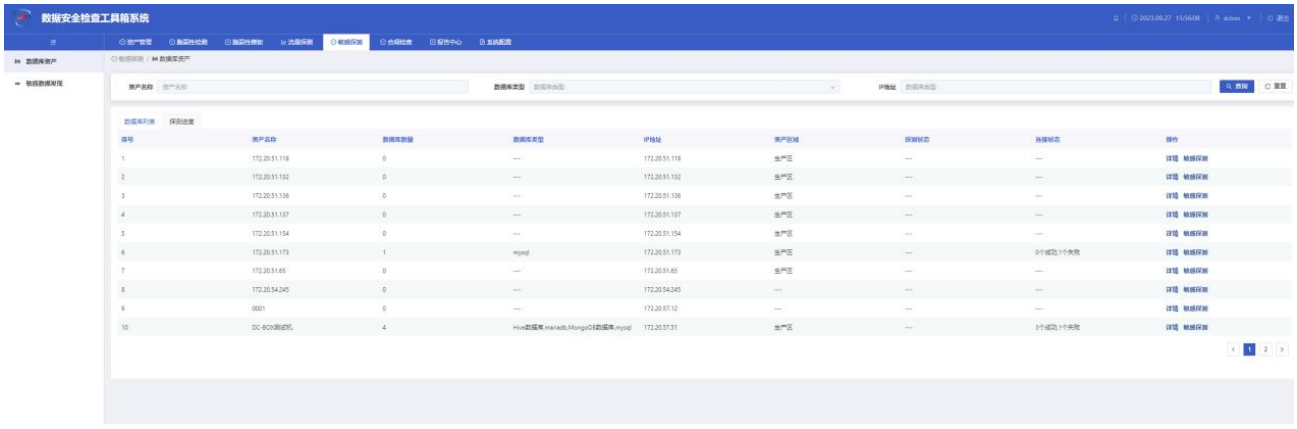


图 7.1.1-1 数据库列表

点击详情可以配置数据库的详细信息，点击‘点击连接’可以测试是否能正常连接。如果连接成功，下方的统计会显示数据库的详细信息。

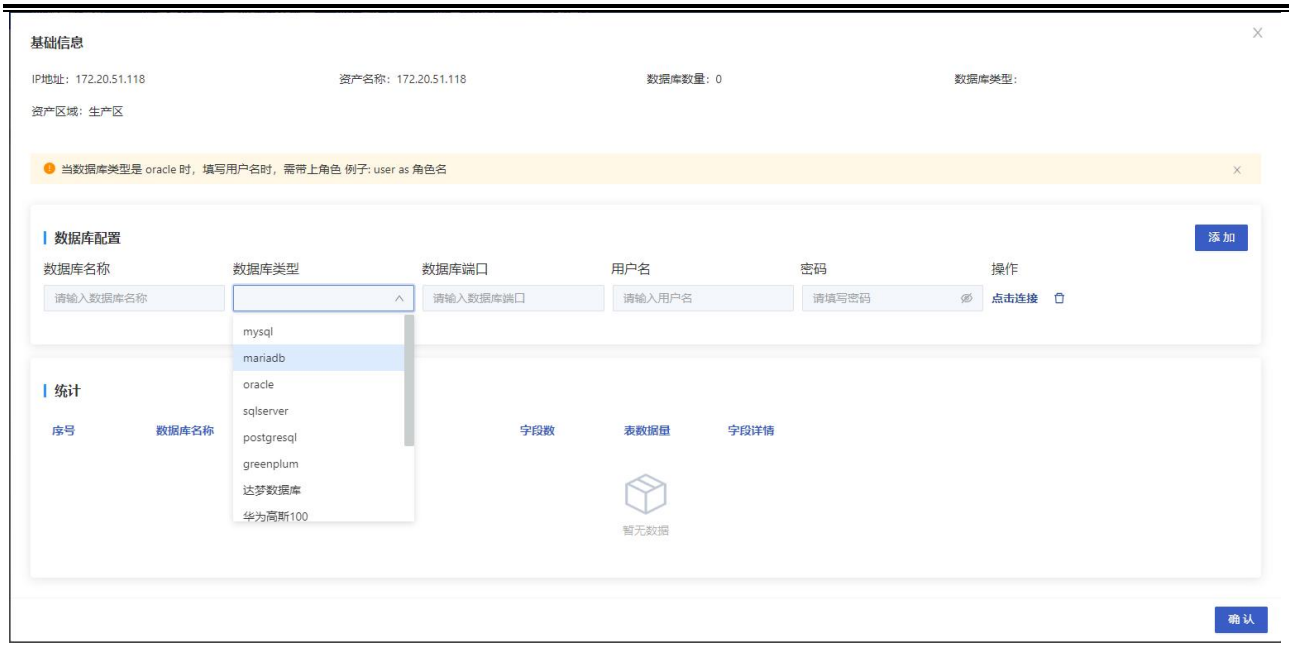


图 7.1.1-2 添加数据库资产

参数	说明
数据库名称	显示当前任务的名称
数据库类型	选择的类型有 mysql、mariadb、oracle、sqlserver、postgresql、greenplum、达梦数据库、华为高斯 100、TIDB、巨杉数据库、Hive 数据库、MongoDB 数据库
数据库端口	根据不用的数据库类型来输入相应的端口
用户名	输入数据库的用户名
密码	输入数据库的密码

如果有连接成功的数据库，此时点击敏感探测就可以对数据库进行敏感数据扫描。

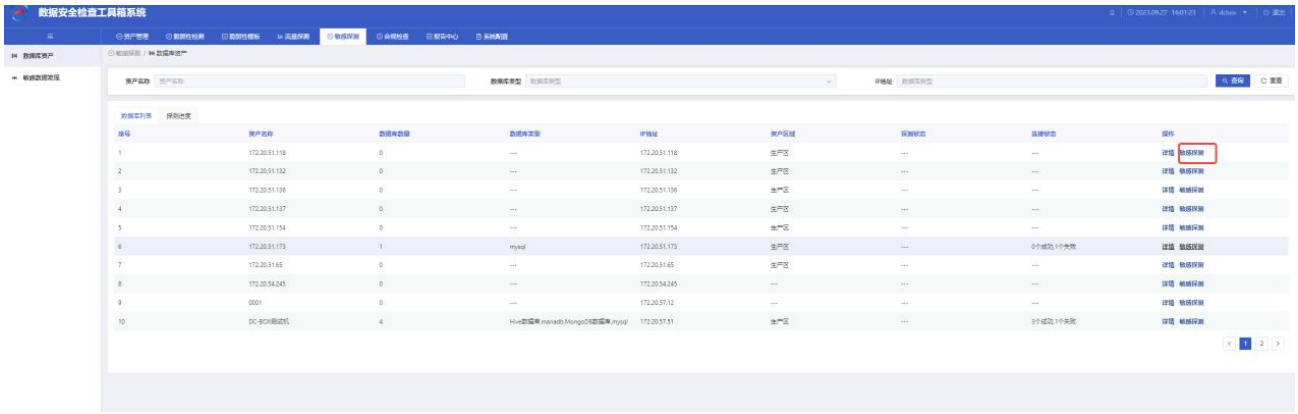


图 7.1.1-3 敏感探测

7.1.2 探测进度

WEBUI：主界面 -> 敏感探测 -> 数据库资产-> 探测进度

点击了敏感探测的数据库会在这里显示进度。点击“开始”，重新进行敏感探测。探测中的资产，点击“终止”，暂停对应的敏感探测。

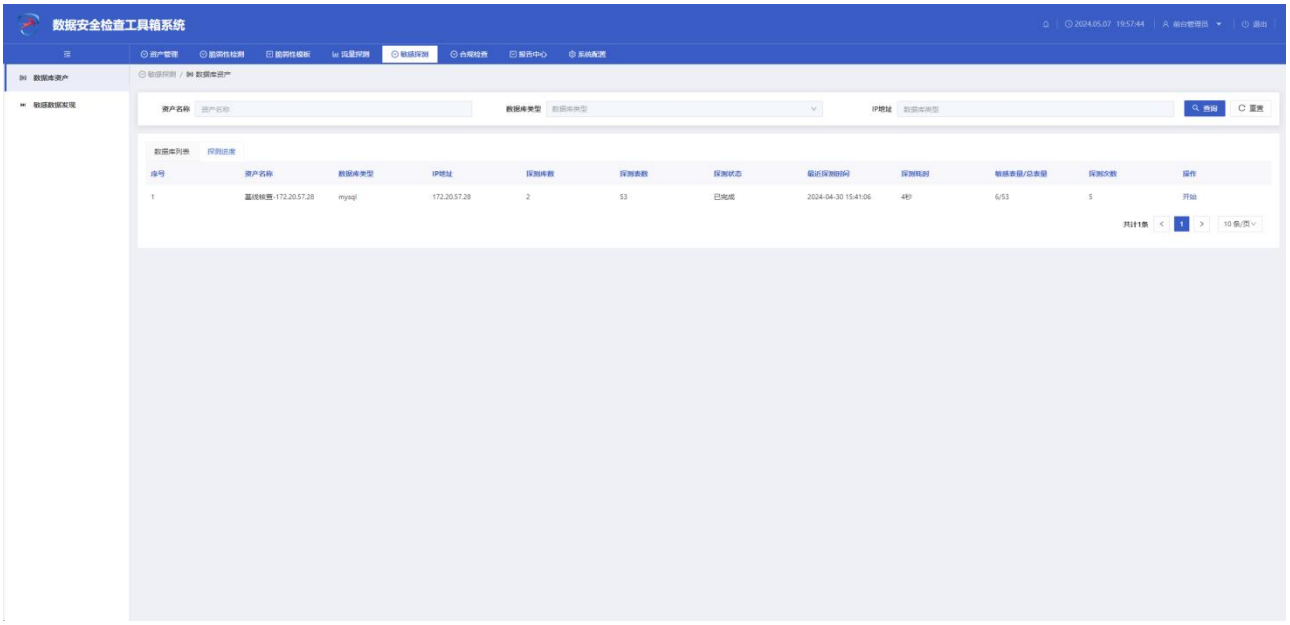


图 7.1.2 探测进度

7.2 敏感数据发现

WEBUI：主界面 -> 敏感探测 -> 敏感数据发现

已经敏感探测完的数据会在这里进行展示。数据库检索可以选择想要展示的数据库。

下方的敏感表导出可以导出具体的敏感字段。

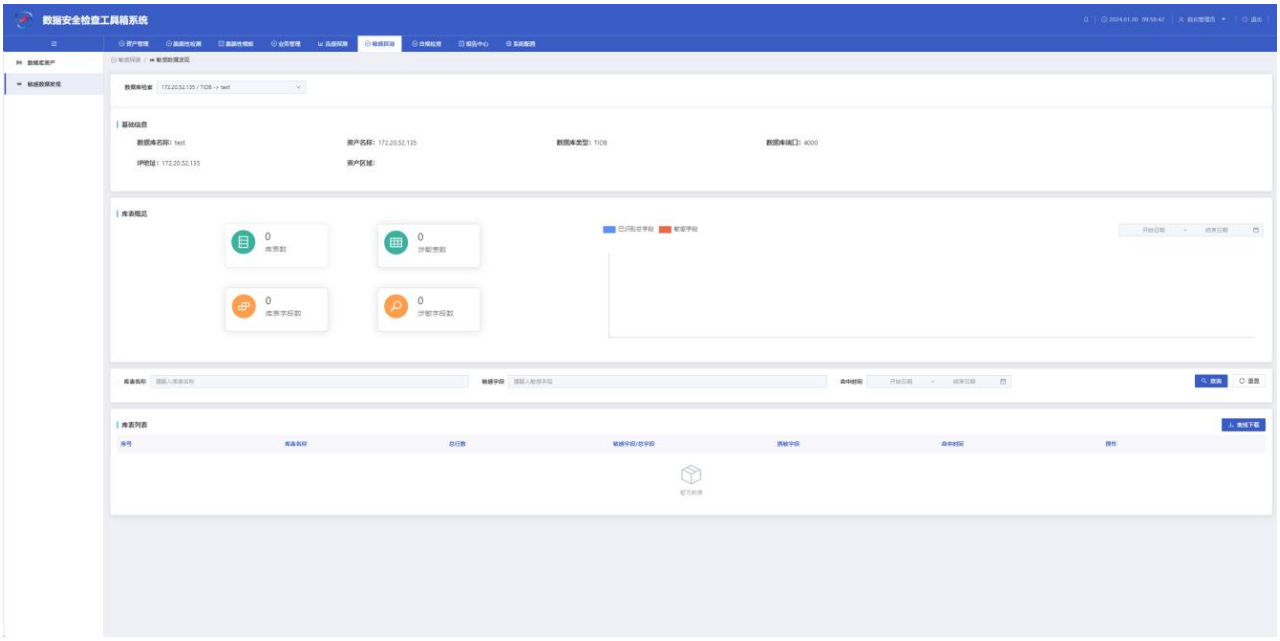


图 7.2-1 敏感数据发现结果

也可以通过检索后来导出所要查询的敏感表，导出的内容是检索后的全部库表，具体方法：输入检索条件后，点击查询，库表列表显示信息后，点击离线下载，最后输入任务名称，点击创建任务即可。

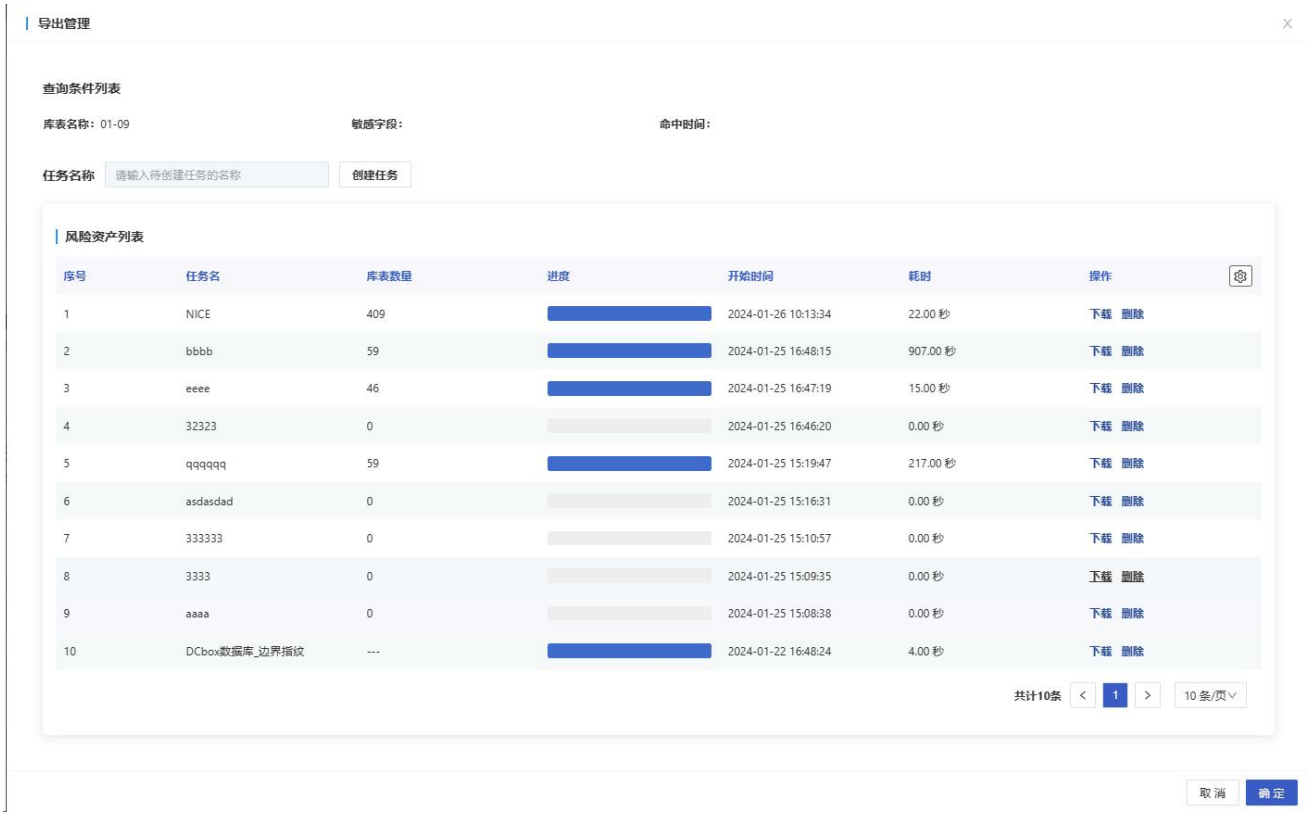


图 7.2-2 离线下载

八. 合规检查

8.1 法规合规检查

WEBUI：主界面 -> 合规检查 -> 法规合规检查

进入法规合规检查页面，可以查看当前支持检查的法规列表

图 8.1-1 法律法规检查

点击“取证原文”，可以查看流量探测中命中相应法规的任务详情信息，点击“复测”按钮，会重新启动相关的流量探测任务。

图 8.1-2 取证原文

8.2 知识库

WEBUI：主界面 -> 合规检查 -> 知识库

进入知识库页面，可查看具体的法规列表及详情信息，列表可根据法规标准分类、法规标准细则分类进行检索查询。

图 8.2 知识库

九. 报告中心

9.1 资产报告导出

WEBUI：主界面 -> 报告中心 -> 资产报告导出

资产报告导出可导出资产台账全览、流量报告导出、综合报告导出内容，导出完成后，下方历史导出记录同步新增一条导出记录。

点击“报告下载”，可下载已有记录的报告。

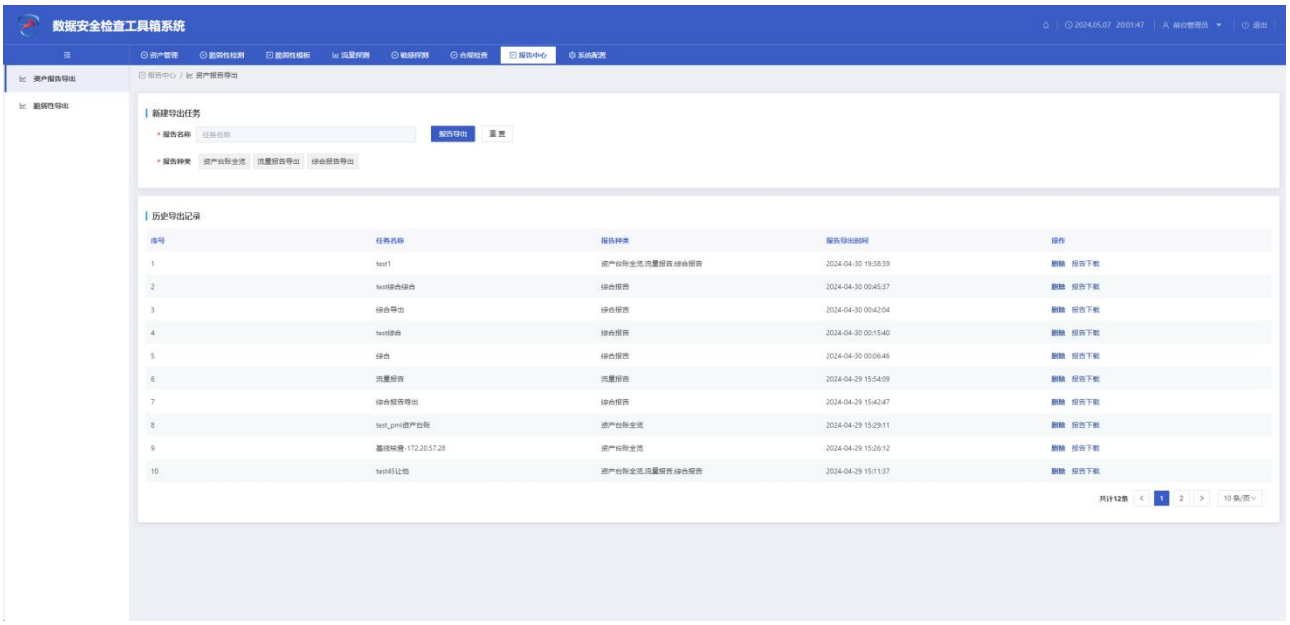


图 9.1 资产报告导出

9.2 脆弱性导出

WEBUI：主界面 -> 报告中心 ->脆弱性导出

报表导出主要是针对多个用户角色生成多种类型的报表，以图、表、文字描述相结合的方式展示给用户。

9.2.1 输出报表

用户可将漏洞扫描结果以报表的形式进行输出。可选择导出对象、资产组以及检测任务时间段。导出格式提供了 HTML，WORD，PDF ,EXCEL，XML 五种格式，导出方式分为详细报告和统计报表，报表标题可自定义，导出文件名默认同步资产名称，也可对其进行自定义，报表内容支持使用报表模板进行自定义，也支持压缩包加密功能。

导出报表操作如下：

1） 选择菜单导出报表->导出报表，进入报表导出页面，如下

图 9.2.1-1 导出报表

2）选择配置导出的报表参数，如下

表 9.2.1-1 导出报表参数说明

参数	说明
选择导出对象	可选择按照任务或者按照资产导出报表
指定任务列表/资产	可选择任务和已生成的资产
任务历史执行时间	开启可选择该任务某次扫描的结果
导出格式	支持 HTML、WORD、EXCEL、PDF、XML 五种报表格式
导出方式	分为详细报表和统计报表两种
报表标题	可自定义报表标题，也可使用默认标题
导出文件名	可自定义导出文件名，也可使用默认名称
设置压缩报密码	导出报表压缩包支持设置压缩密码，通常在涉密机构使用

1)点击导出，跳转到报表列表界面，展示导出的进度

图 9.2.1-2 导出报表

2）报表导出成功后可在报表列表点击下载

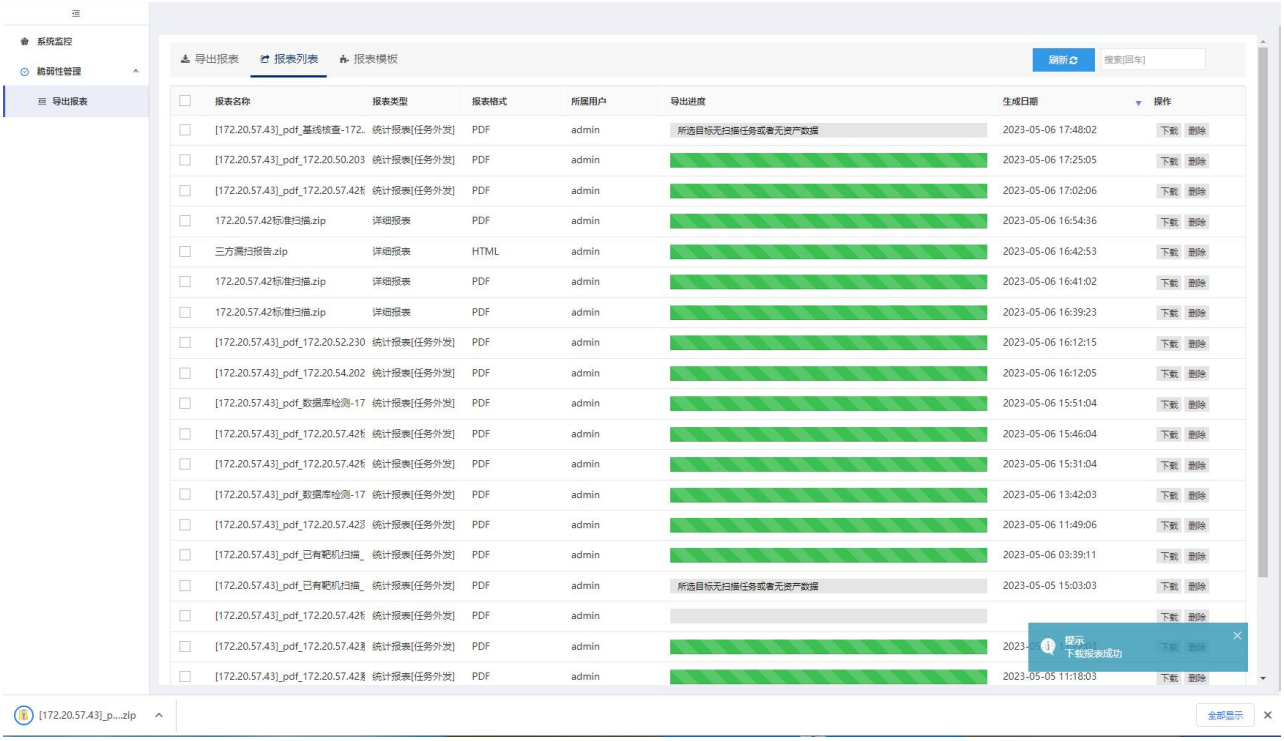


图 9.2.1-3 导出报表完成

9.2.2 报表列表

报表列表是将导出的报表直接同步到报表列表里，报表列表可以展示导出的报表名称以及生成日期，报表名称默认包含扫描类型、资产以及报表格式。报表格式可以存储多个报表文件，若报表列表里面报表较多，查找不方便，可通过搜索名称来进行搜索。对于报表文件支持批量删除，以及单报表删除。具体详情如下图 10.2.2-1 所示

图 9.2.2-1 报表列表

9.2.3 报表详情

资产报表内容由主机资产和主机上的 web 资产信息组成，报表数据来自系统扫描、web 扫描、口令猜解、存活探测扫描任务的扫描结果；报表按内容分为统计报表和详细报表

9.2.3.1 统计报表

统计报表：内容包括按任务或者按资产导出的经扫描后的数据统计信息，如检测结果综述、任务概览、漏洞统计、敏感端口/服务/中间件、漏洞分布、类别统计等。具体详情如下图所示：

1 检测结果综述

本次检测中，扫描了1个主机，17个站点。
检测到漏洞共1398个，系统漏洞897个，Web漏洞501个。高危漏洞共344个，中危漏洞共517个，低危漏洞共480个，信息级漏洞共57个。
检测到弱口令共0个。
整体风险等级为 非常危险，非常危险的资产共7个，需重点关注。

2 任务总体概览

2.1 任务基本信息

任务名称	172.20.50.203
扫描目标	172.20.50.203
报表模板	默认模板
任务所在账号	admin
扫描时间	系统扫描：2023-05-06 15:43:18 至 2023-05-06 16:01:14 (耗时：17分56秒) Web扫描：2023-05-06 16:01:21 至 2023-05-06 17:24:29 (耗时：1小时23分) 口令猜解: 2023-05-06 16:01:21 至 2023-05-06 16:30:55 (耗时：29分34秒)
系统版本	V3.0(6.6.1-R1-v90757-20230222)
规则库版本	20230417151610

2.2 敏感端口/服务

本次任务检测到开放了以下【21】种敏感端口或服务，开放最多的端口为【137】端口，对应【2】个资产，具体情况如下表所示。

序号	端口	服务	协议	主机
1	21	ftp	TCP	172.20.50.203
2	22	ssh/WeOnlyDo sshd 2.4.3	TCP	172.20.50.203
3	23	telnet/Microsoft Windows XP telnetd	TCP	172.20.50.203
4	80	http/Microsoft HTTPAPI httpd 2.0	TCP	172.20.50.203
5	135	msrpc/Microsoft Windows RPC	TCP	172.20.50.203
6	137	netbios-ns	TCP	172.20.50.203
7	137	netbios-ns/Microsoft Windows netbios-ns	UDP	172.20.50.203
8	139	netbios-ssn/Microsoft Windows netbios-ssn	TCP	172.20.50.203
9	443	https/apache:http_server:2.4.46 Apache httpd	TCP	172.20.50.203
10	445	microsoft-ds/Microsoft Windows 7 - 10 microsoft-ds	TCP	172.20.50.203
11	1433	ms-sql-s/microsoft:sql_server:2008_r2:gold Microsoft SQL Server 2008 R2	TCP	172.20.50.203
12	1521	oracle-tns/Oracle TNS	TCP	172.20.50.203
13	3306	mysql/mysql:mysql:5.6.50 MySQL	TCP	172.20.50.203
14	3389	ms-wbt-server/TLSv1	TCP	172.20.50.203
15	5432	postgresql/postgresql:postgresql:9.6 PostgreSQL DB	TCP	172.20.50.203
16	5466	http	TCP	172.20.50.203
17	5677	http	TCP	172.20.50.203
18	7756	http	TCP	172.20.50.203
19	8080	http/apache:http_server:2.4.46 Apache httpd	TCP	172.20.50.203
20	8088	http	TCP	172.20.50.203
21	56777	http	TCP	172.20.50.203

说明：敏感端口/服务根据安全研究表明，容易被黑客利用漏洞发起攻击的端口/服务。

目录

2.3 敏感中间件

本次任务检测到以下种敏感中间件，其中使用最多的中间件是【】，具体情况如下表所示：

序号	中间件	网站

说明：敏感中间件是指安全研究表明，容易被黑客利用发起攻击的中间件。

3 资产信息统计

3.1 端口/服务统计

资产的端口/服务开放情况如下表所示，开放端口最多的资产为【172.20.50.203】，共开放了【45】个端口：

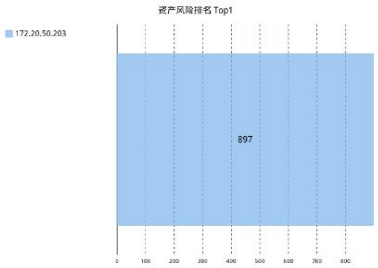
序号	主机名	端口/"服务"/协议	端口总数
1	172.20.50.203	21/"ftp"/"TCP" 22/"ssh/WeOnlyDo sshd 2.4.3"/"TCP" 23/"telnet/Microsoft Windows XP telnetd "/"TCP" 80/"http/Microsoft HTTPAPI httpd 2.0"/"TCP" 135/"msrpc/Microsoft Windows RPC "/"TCP" 137/"netbios-ns"/"TCP" 137/"netbios-ns/Microsoft Windows netbios-ns "/"UDP" 139/"netbios-ssn/Microsoft Windows netbios-ssn "/"TCP" 443/"https/apache:http_server:2.4.46 Apache httpd"/"TCP" 445/"microsoft-ds/Microsoft Windows 7 - 10 microsoft-ds "/"TCP" 1025/"msrpc/Microsoft Windows RPC "/"TCP" 1026/"LSA-or-nterm"/"TCP" 1027/"msrpc/Microsoft Windows RPC "/"TCP" 1028/"unknown"/"TCP" 1048/"neod2"/"TCP" 1070/"gmrupdateserv"/"TCP" 1074/"warmspotMgmt"/"TCP" 1128/"saphostctrl"/"TCP" 1136/"hhb-gateway"/"TCP" 1433/"ms-sql-s/microsoft:sql_server:2008_r2:gold Microsoft SQL Server 2008 R2"/"TCP" 1468/"csdm"/"TCP" 1521/"oracle-tns/Oracle TNS "/"TCP" 2383/"ms-olap4"/"TCP" 3300/"ceph"/"TCP" 3306/"mysql/mysql:mysql:5.6.50 MySQL"/"TCP" 3389/"ms-wbt-server/TLSv1 "/"TCP" 3638/"ehp-backup"/"TCP" 5357/"http/Microsoft HTTPAPI httpd 2.0"/"TCP" 5432/"postgresql/postgresql:postgresql:9.6 PostgreSQL DB"/"TCP" 5466/"http"/"TCP" 5500/"oracle/https/oracle:database_server:::enterprise Oracle XML DB Enterprise Edition httpd"/"TCP" 5677/"http"/"TCP" 5985/"http/Microsoft HTTPAPI httpd 2.0"/"TCP" 7756/"http"/"TCP" 8000/"http/apache:http_server:2.2.8 Apache httpd"/"TCP" 8080/"http/apache:http server:2.4.46 Apache httpd"/"TCP"	45

目录

3.2 资产风险等级

3.2.1 主机资产风险

主机资产风险等级分布（TOP10）如下图所示。

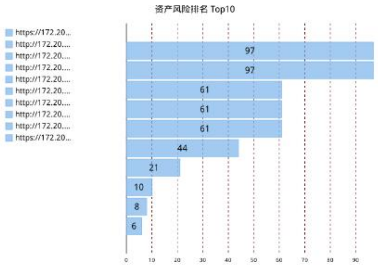


所有主机资产的页面数、漏洞及风险情况如下表所示。

序号	IP地址	高	中	低	信息	总计	风险值	资产风险等级
1	172.20.50.203	335	436	105	21	897	10.0	非常危险

3.2.2 WEB资产风险

Web资产风险等级分布（TOP10）如下图所示



所有Web资产的页面数、漏洞及风险情况如下表所示。

序号	资产URL	页面数	高	中	低	信息	总计	风险值	资产风险等级
1	http://172.20.50.203:8000/	321	3	8	25	8	44	9.3	非常危险
2	http://172.20.50.203:8085/	1	2	1	6	1	10	9.0	非常危险
3	http://172.20.50.203:56777/	26	1	1	58	1	61	8.0	非常危险
4	http://172.20.50.203:5677/	26	1	1	58	1	61	8.0	非常危险
5	http://172.20.50.203:7756/	26	1	1	58	1	61	8.0	非常危险
6	http://172.20.50.203:8093/	1	1	0	6	1	8	8.0	非常危险
7	https://172.20.50.203/	704	0	34	55	8	97	7.9	比较危险
8	http://172.20.50.203:8080/	704	0	34	55	8	97	7.9	比较危险
9	http://172.20.50.203:8088/	813	0	1	19	1	21	5.0	比较危险

目录

4 漏洞信息统计

4.1 受影响资产统计

4.1.1 系统漏洞影响资产

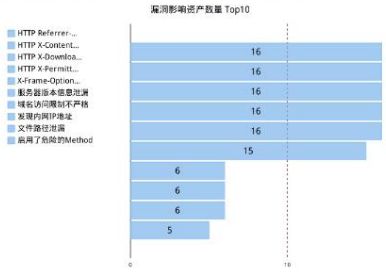
影响主机资产最多的漏洞是【**Adobe Shockwave Player 缓冲区错误漏洞（CVE-2011-2124）**】，共有【**1**】主机中存在该漏洞，漏洞等级为高风险。漏洞影响资产数量TOP10分布如下图所示：

系统漏洞影响主机资产数量TOP10如下表所示。

序号	漏洞名称	漏洞分组	受影响资产
1	Adobe Shockwave Player 缓冲区错误漏洞（CVE-2011-2124）	缓冲区溢出	172.20.50.203
2	Apache Commons Configuration 输入验证错误漏洞（CVE-2020-1953）	输入验证	172.20.50.203
3	Apache HTTP Server httpoxy 安全漏洞（CVE-2016-5387）	访问控制	172.20.50.203
4	Apache HTTP Server 代码问题漏洞（CVE-2021-26690）	代码问题	172.20.50.203
5	Apache HTTP Server 代码问题漏洞（CVE-2021-34798）	代码问题	172.20.50.203
6	Apache HTTP Server 代码问题漏洞（CVE-2021-44224）	代码问题	172.20.50.203
7	Apache HTTP Server 信息泄露漏洞（CVE-2022-30556）	信息泄露	172.20.50.203
8	Apache HTTP Server 安全漏洞（CVE-2016-8743）	代码问题	172.20.50.203
9	Apache HTTP Server 安全漏洞（CVE-2021-33193）	其它	172.20.50.203
10	Apache HTTP Server 数据伪造问题漏洞（CVE-2022-31813）	数据伪造	172.20.50.203

4.1.2 WEB漏洞影响资产

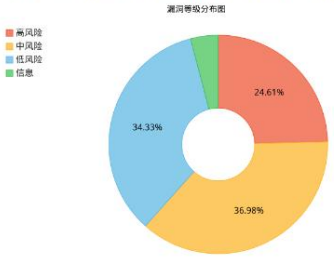
影响Web资产最多的漏洞是【**HTTP Referrer-Policy头缺失**】，共有【**16**】个Web站点中存在该漏洞，漏洞等级为【低风险】。漏洞影响资产数量TOP10分布如下图所示：



目录

4.2 漏洞等级分布

本次任务中，漏洞按高、中、低、信息等级分布结构如下图所示。出现次数最多的是【**中风险**】漏洞，共【**517**】次，占全部漏洞的【**36.98%**】，漏洞等级分布图如下所示：



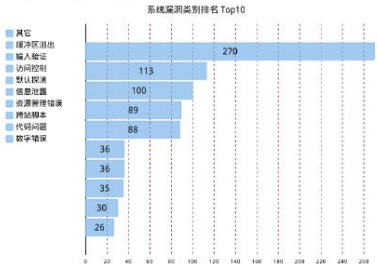
按漏洞风险等级统计具体情况如下表所示：

	高	中	低	信息	总计（次）
系统漏洞	335	436	105	21	897
WEB漏洞	9	81	375	36	501
总计（次）	**344**	**517**	**480**	**57**	**1398**

4.3 漏洞类别统计

4.3.1 系统漏洞类别

所有系统漏洞中，出现次数最多的漏洞类型是【**其它：270个**】，具体漏洞类别分布如下图所示：



本次任务中，所有系统漏洞类型统计情况如下表所示：

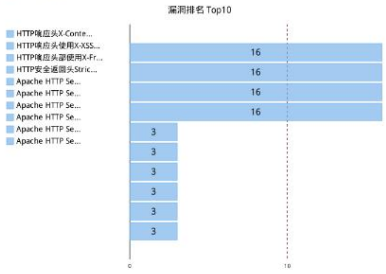
序号	系统漏洞类别	总计（次）
1	其它	270
2	缓冲区溢出	113
3	输入验证	100
4	访问控制	89
5	默认探测	88
6	信息泄露	36
7	资源管理错误	36

目录

4.4 漏洞排名

4.4.1 系统漏洞TOP10

按漏洞名称排序，系统漏洞发现次数TOP10分布情况如下图所示：

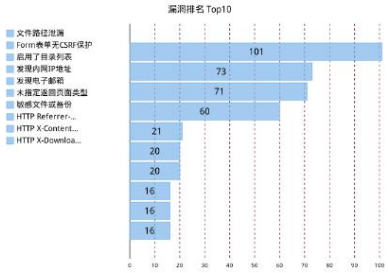


系统漏洞出现次数TOP10如下表所示：

序号	系统漏洞名称	漏洞分组	总计（次）
1	HTTP响应头X-Content-Options：nosniff检查	默认探测	16
2	HTTP响应头使用X-XSS-Protection检查	默认探测	16
3	HTTP响应头部使用X-Frame-Options检查	默认探测	16
4	HTTP安全返回头Strict-Transport-Security检查	默认探测	16
5	Apache HTTP Server 代码问题漏洞（CVE-2021-34798）	代码问题	3
6	Apache HTTP Server 信息泄露漏洞（CVE-2022-30556）	信息泄露	3
7	Apache HTTP Server 数据伪造问题漏洞（CVE-2022-31813）	数据伪造	3
8	Apache HTTP Server 环境问题漏洞（CVE-2022-22720）	环境条件	3
9	Apache HTTP Server 缓冲区错误漏洞（CVE-2021-39275）	缓冲区溢出	3
10	Apache HTTP Server 缓冲区错误漏洞（CVE-2021-44790）	缓冲区溢出	3

4.4.2 WEB漏洞TOP10

按漏洞名称排序，Web漏洞发现次数TOP10分布情况如下图所示：



Web漏洞出现次数TOP10如下表所示：

序号	漏洞名称	漏洞分组	总计（次）

目录

5 弱口令

序号	主机地址	用户名	密码	服务	端口

6 历史检测详情

本次任务历史检测结果变化趋势如下图所示：

具体历史检测时间段及漏洞结果总计如下表所示：

任务类型	开始时间	结束时间	漏洞总计
系统扫描	2023-05-06 15:43:18	2023-05-06 16:01:14	897
弱口令扫描	2023-05-06 16:01:21	2023-05-06 16:30:55	0
WEB扫描	2023-05-06 16:01:21	2023-05-06 17:24:29	501

7 参考标准

7.1 单一漏洞风险等级评定标准

危险程度	危险值区域	危险程度说明
高	7 <= 漏洞风险值 <= 10	攻击者可以访问机密信息、破坏或删除数据且可以制造系统中断。
中	4 <= 漏洞风险值 < 7	攻击者可访问部分受限的信息、可以破坏信息且可以禁用网络中的个体目标系统。
低	0 < 漏洞风险值 < 4	攻击者可以在特殊情况下访问不受限的信息、破坏或损坏信息但无法制造任何系统中断。
信息	漏洞风险值 = 0	攻击者可以获取服务及组件等版本信息。

1. 可远程获取漏洞组件的版本信息。
2. 目标系统服务器开放了不必要的服务。
3. 可远程访问到某些不在目录树中的文件或读取服务器动态脚本的源码。
4. 可远程因为会话管理的问题导致身份冒用。
5. 可远程利用受影响的系统服务器攻击其他浏览网站的用户。
6. 可远程读取系统文件或后台数据库。
7. 可远程读写系统文件、操作后台数据库。
8. 可远程以普通用户身份执行命令或进行拒绝服务攻击。
9. 可远程以管理用户身份执行命令（受限、不太容易利用）。
10. 可远程以管理用户身份执行命令（不受限、容易利用）。

7.2 资产风险等级评定标准

资产风险等级	资产风险值区域
非常危险	8 <= 资产风险值 <= 10
比较危险	5 <= 资产风险值 < 8
比较安全	2 <= 资产风险值 < 5
非常安全	0 <= 资产风险值 < 2

1. 将资产的漏洞按照分数的高低排序，依据漏洞的分数将漏洞威胁划分为高、中、低三个类别。
2. 单个资产的风险值按照风险评估模型计算来得到；网络的风险值是由最危险资产决定，即最大的资产风险值。
3. 高、中、低漏洞威胁的定义参见《单一漏洞风险等级评定标准》。
4. 资产的风险等级定位为四级：非常危险、比较危险、比较安全和非常安全。具体的评判标准请参考《资产风险等级评定标准》。

8 安全建议

随着越来越多的网络访问通过系统漏洞进行操作，系统漏洞已成为互联网安全的一个热点，基于系统漏洞的攻击广为流行，CGI攻击检测、网络设备和防火墙、本地安全检查等问题严重威胁着系统管理者和系统用户的安全，我们有必要采取措施消除这些风险。

建议对存在漏洞的资产参考附件中提出的解决方案进行漏洞修补、安全增强。

请专业的安全研究人员或安全公司对系统架构做全面的安全审计，修补所有发现的安全漏洞，这种白盒安全测试比较深入全面。

对系统的开发人员进行安全编码方面的培训，在开发过程避免漏洞的引入能起到事半功倍的效果。

采用专业的系统安全产品，可以在不修改系统本身的情况下对大多数的基于漏洞攻击起到有效的阻断作用。

建议网络管理员、系统管理员、安全管理员关注安全信息、安全动态及最新的高危漏洞，特别是影响到漏洞站点所使用的系统和软件的漏洞，应该在事前设计好应对规划，一旦发现系统受漏洞影响及时采取措施。

9 联系我们

公司：熙羚信息技术有限公司
网址：https://www.xilinginfo.com/
热线：0571-86955515
传真：support@seclead.cn
地址：浙江省杭州市滨江区长河街道滨康路352号中控信息大厦B2505

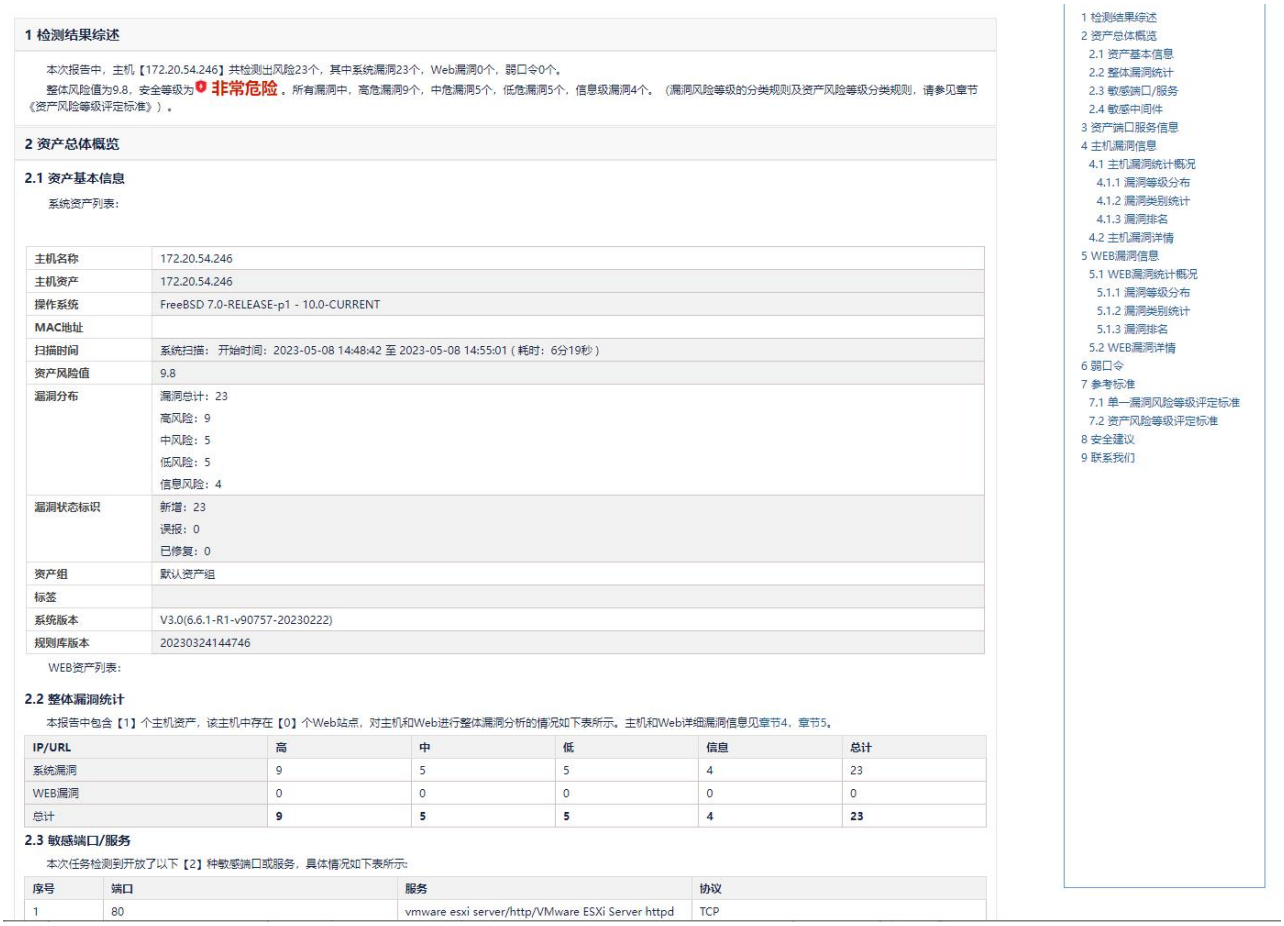
目录

图 9.2.3.1-1 统计报表内容

：html、word、pdf 格式报表内容相同，只是以不同形式展示出来，建议用户导出报表为 html，排版更加直观美观。

9.2.3.2 详细报表

详细报表：导出的详细报表压缩包中包含所选任务或者所选资产的统计报表和每个资产的详细报表，详细报表中展示了资产和任务的详细信息，如资产检测时间、检测结果详情、资产属性信息、详细的漏洞描述信息等，如下图所示：



1 检测结果综述

本次报告中，主机【172.20.54.246】共检测出风险23个，其中系统漏洞23个，Web漏洞0个，弱口令0个。

整体风险值为9.8，安全等级为 非常危险 。所有漏洞中，高危漏洞9个，中危漏洞5个，低危漏洞5个，信息级漏洞4个。（漏洞风险等级的分类规则及资产风险等级分类规则，请参见章节《资产风险等级评定标准》）。

2 资产总体概览

2.1 资产基本信息

系统资产列表：

主机名称	172.20.54.246
主机资产	172.20.54.246
操作系统	FreeBSD 7.0-RELEASE-p1 - 10.0-CURRENT
MAC地址	
扫描时间	系统扫描： 开始时间：2023-05-08 14:48:42 至 2023-05-08 14:55:01 (耗时：6分19秒)
资产风险值	9.8
漏洞分布	漏洞总计：23 高风险：9 中风险：5 低风险：5 信息风险：4
漏洞状态标识	新增：23 误报：0 已修复：0
资产组	默认资产组
标签	
系统版本	V3.0(6.6.1-R1-v90757-20230222)
规则库版本	20230324144746

WEB资产列表：

2.2 整体漏洞统计

本报告中包含【1】个主机资产，该主机中存在【0】个Web站点，对主机和Web进行整体漏洞分析的情况如下表所示。主机和Web详细漏洞信息见章节4，章节5。

IP/URL	高	中	低	信息	总计
系统漏洞	9	5	5	4	23
WEB漏洞	0	0	0	0	0
总计	**9**	**5**	**5**	**4**	**23**

2.3 敏感端口/服务

本次任务检测到开放了以下【2】种敏感端口或服务，具体情况如下表所示：

序号	端口	服务	协议
1	80	vmware esxi server/http/VMware ESXi Server httpd	TCP

说明：敏感端口/服务指根据安全研究表明，容易被黑客利用漏洞发起攻击的端口/服务。

2.4 敏感中间件

本次任务检测到以下【0】种敏感中间件，具体情况如下表所示：

序号	中间件

说明：敏感中间件是指安全研究表明，容易被黑客利用发起攻击的中间件。

3 资产端口服务信息

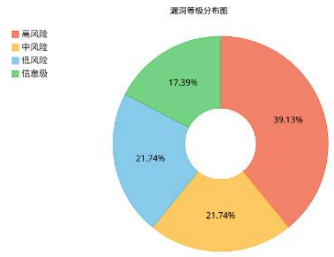
资产的端口/服务开放情况如下表所示，共开放了【7】个端口：

端口	服务	协议	漏洞总数
⊞ 80	vmware esxi server/http/VMware ESXi Server httpd	TCP	5
427	svrloc/Service Location Protocol 2	UDP	0
⊞ 443	https	TCP	16
⊞ 902	iss-realsecure/VMware Authentication Daemon 1.10	TCP	1
8000	http-alt	TCP	0
8300	tmi	TCP	0
9080	soap/genivia:gsoap:2.8 gSOAP	TCP	0
⊞ --	--	ICMP	1

4 主机漏洞信息

4.1 主机漏洞统计概况

4.1.1 漏洞等级分布



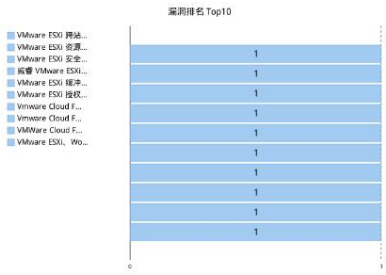
高风险	中风险	低风险	信息级	总计
9	5	5	4	23

4.1.2 漏洞类别统计

序号	主机漏洞类别（TOP10）	总计
1	跨站脚本	14
2	默认探测	7
3	其它	1
4	Web应用	1

目录

4.1.3 漏洞排名



序号	系统漏洞名称（TOP10）	总计
1	VMware ESXi 跨站脚本漏洞（CVE-2020-3955）	1
2	VMware ESXi 资源管理错误漏洞（CVE-2020-4004）	1
3	VMware ESXi 安全漏洞（CVE-2020-4005）	1
4	威睿 VMware ESXi 缓冲区错误漏洞（CVE-2021-21974）	1
5	VMware ESXi 缓冲区错误漏洞（CVE-2021-21995）	1
6	VMware ESXi 授权问题漏洞（CVE-2021-21994）	1
7	Vmware Cloud Foundation 资源管理错误漏洞（CVE-2021-22050）	1
8	Vmware Cloud Foundation 输入验证错误漏洞（CVE-2021-22043）	1
9	VMWare Cloud Foundation (ESXi) 访问控制错误漏洞（CVE-2021-22042）	1
10	VMware ESXi、Workstation和Fusion 安全漏洞（CVE-2018-6972）	1

4.2 主机漏洞详情

漏洞名称	漏洞分类	漏洞类型	出现次数
VMware ESXi 跨站脚本漏洞（CVE-2020-3955）	跨站脚本	高风险	1
VMware ESXi 资源管理错误漏洞（CVE-2020-4004）	资源管理错误	高风险	1
VMware ESXi 安全漏洞（CVE-2020-4005）	其它	高风险	1
威睿 VMware ESXi 缓冲区错误漏洞（CVE-2021-21974）	缓冲区溢出	高风险	1
VMware ESXi 缓冲区错误漏洞（CVE-2021-21995）	缓冲区溢出	高风险	1
VMware ESXi 授权问题漏洞（CVE-2021-21994）	授权问题	高风险	1
Vmware Cloud Foundation 资源管理错误漏洞（CVE-2021-22050）	资源管理错误	高风险	1
Vmware Cloud Foundation 输入验证错误漏洞（CVE-2021-22043）	输入验证	高风险	1
VMWare Cloud Foundation (ESXi) 访问控制错误漏洞（CVE-2021-22042）	访问控制	高风险	1
VMware ESXi、Workstation和Fusion 安全漏洞（CVE-2018-6972）	代码问题	中风险	1
多款Intel产品信息泄露漏洞（CVE-2018-3646）	信息泄露	中风险	1
VMware ESXi 资源管理错误漏洞（CVE-2020-3976）	资源管理错误	中风险	1

目录

5.1 WEB漏洞统计概况

5.1.1 漏洞等级分布

高风险	中风险	低风险	信息级	总计
0	0	0	0	0

5.1.2 漏洞类别统计

序号	WEB漏洞类别	总计

5.1.3 漏洞排名

序号	WEB漏洞名称（TOP10）	总计

5.2 WEB漏洞详情

漏洞名称	漏洞分类	漏洞类型	出现次数

6 弱口令

序号	主机地址	用户名	密码	服务	端口

目录

7 参考标准

7.1 单一漏洞风险等级评定标准

危险程度	危险值区域	危险程度说明
高	7 <= 漏洞风险值 <= 10	攻击者可以访问机密信息、破坏或删除数据且可以制造系统中断。
中	4 <= 漏洞风险值 < 7	攻击者可访问部分受限的信息、可以破坏信息且可以禁用网络中的个体目标系统。
低	0 < 漏洞风险值 < 4	攻击者可以在特殊情况下访问不受限的信息、破坏或损坏信息但无法制造任何系统中断。
信息	漏洞风险值 = 0	攻击者可以获取服务及组件等版本信息。

1. 可远程获取漏洞组件的版本信息。
2. 目标系统服务器开放了不必要的服务。
3. 可远程访问到某些不在目录树中的文件或读取服务器动态脚本的源码。
4. 可远程因为会话管理的问题导致身份冒用。
5. 可远程利用受影响的系统服务器攻击其他浏览网站的用户。
6. 可远程读取系统文件或后台数据库。
7. 可远程读写系统文件、操作后台数据库。
8. 可远程以普通用户身份执行命令或进行拒绝服务攻击。
9. 可远程以管理用户身份执行命令（受限、不太容易利用）。
10. 可远程以管理用户身份执行命令（不受限、容易利用）。

7.2 资产风险等级评定标准

资产风险等级	资产风险值区域
非常危险	8 <= 资产风险值 <= 10
比较危险	5 <= 资产风险值 < 8
比较安全	2 <= 资产风险值 < 5
非常安全	0 <= 资产风险值 < 2

1. 将资产的漏洞按照分数的高低排序，依据漏洞的分数将漏洞威胁划分为高、中、低三个类别。
2. 单个资产的风险值按照风险评估模型计算来得到：网络的风险值是由最危险资产决定，即最大的资产风险值。
3. 高、中、低漏洞威胁的定义参见《单一漏洞风险等级评定标准》。
4. 资产的风险等级定位为四级：非常危险、比较危险、比较安全和非常安全。具体的评判标准请参考《资产风险等级评定标准》。

8 安全建议

随着越来越多的网络访问通过系统漏洞进行操作，系统漏洞已成为互联网安全的一个热点，基于系统漏洞的攻击广为流行，CGI攻击检测、网络设备和防火墙、本地安全检查等问题严重威胁着系统管理者和系统用户的安全，我们有必要采取措施消除这些风险。

建议对存在漏洞的资产参考附件中提出的解决方案进行漏洞修补、安全增强。

请专业的安全研究人员或安全公司对系统架构做全面的安全审计，修补所有发现的安全漏洞，这种白盒安全测试比较深入全面。

对系统的开发人员进行安全编码方面的培训，在开发过程避免漏洞的引入能起到事半功倍的效果。

采用专业的系统安全产品，可以在不修改系统本身的情况下对大多数的基于漏洞攻击起到有效的阻断作用。

建议网络管理员、系统管理员、安全管理员关注安全信息、安全动态及最新的高危漏洞，特别是影响到漏洞站点所使用的系统和软件的漏洞，应该在事前设计好应对规划，一旦发现系统受漏洞影响及时采取措施。

9 联系我们

公司：熙羚信息技术有限公司
网址：https://www.xilinginfo.com/
热线：0571-86955515
传真：support@seclead.cn
地址：浙江省杭州市滨江区长河街道滨康路352号中控信息大厦B2505

目录

图 9.2.3.2-1 详细报表内容

9.2.4 报表模板

通过新增报表模板用户可以自定义生成的报表中显示的内容。系统自带了默认模板，默认模板中所有章节内容都开放，不可编辑和删除。

9.2.4.1 新建报表模板

➢自定义漏洞等级、漏洞状态、公司信息、报表标题

操作：（1）点击报表管理->导出报表->报表模板，进入报表模板页面->点击新增，配置模板名字、需要导出的漏洞等级、漏洞状态、公司信息、报表标题，提交，如下：

图 9.2.4.1-1 自定义报表模板

操作：（2）在导出报表页面->选择任务或资产->下拉选择自定义的报表模板->导出，导出的报表内容即和选择的模板一致。如下

图 9.2.4.1-2 选择自定义报表模板导出报表

➢自定义报表章节

操作：（1）点击报表管理->导出报表->报表模板，进入报表模板页面->点击新增，配置模板名字、开启自定义报表章节->选择报表中要展示的章节，提交，如下：

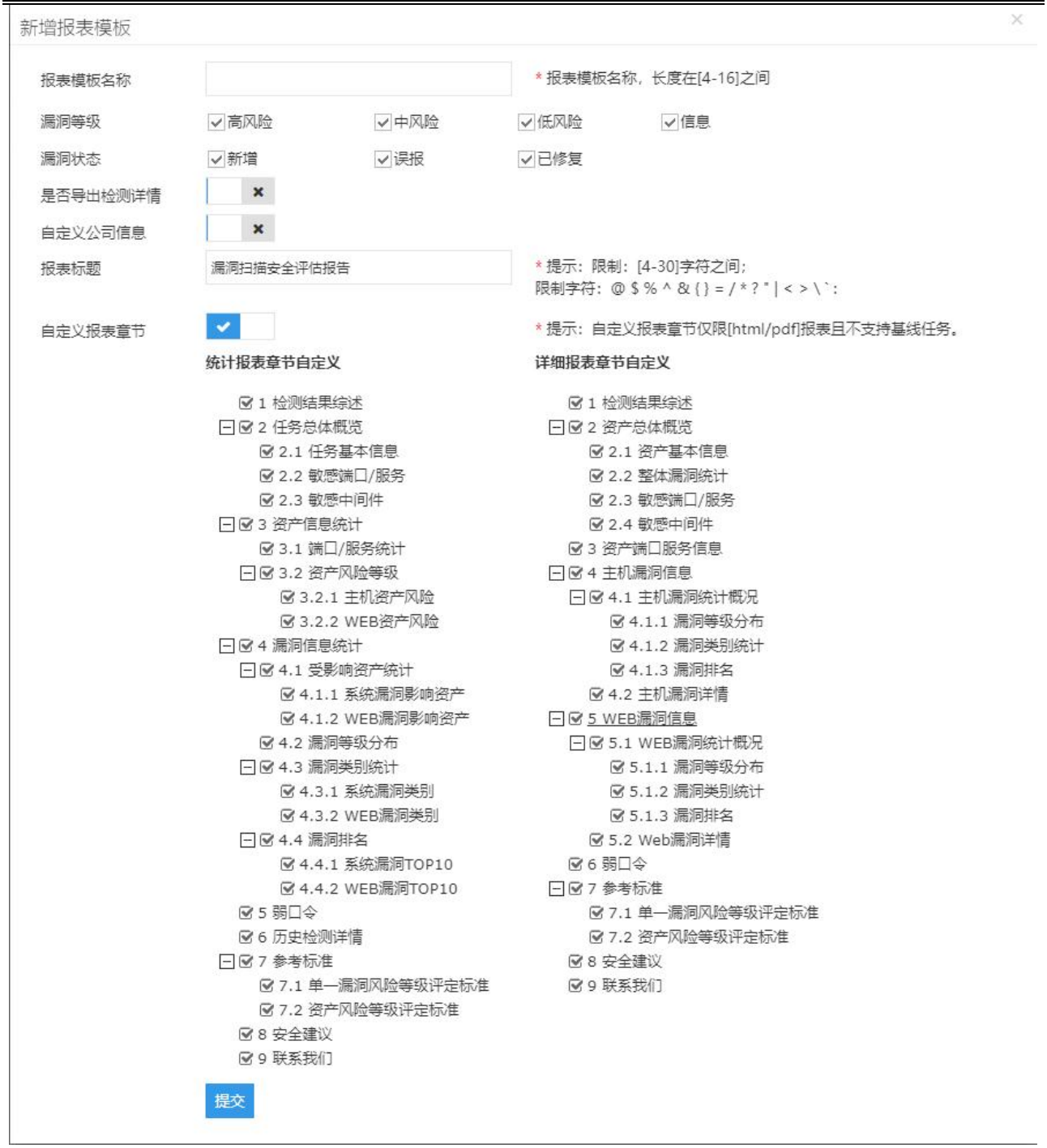


图 9.2.4.1-3 自定义报表章节

操作：（2）在导出报表页面->选择任务或资产->下拉选择自定义的报表模板->导出，导出的报表内容即和选择的模板一致。如下

图 9.2.4.1-4 选择自定义报表章节导出

9.2.4.2 报表模板操作

管理员可以对报表模板中的信息进行编辑和删除操作。

➢**编辑**

操作：选择模板->点击编辑按钮，编辑模板内容后->点击提交，完成模板编辑

➢**删除**

操作：选择模板->点击删除按钮->点击确认，即可删除自定义的模板

9.3 流量探测报告导出

WEBUI：主界面 -> 报告中心 ->流量探测报告导出

流量探测报告导出可导出流量探测界面的所有列表内容，报告可根据探测类型、探测时间、是否安全进行筛选。导出完成后，下方历史导出记录同步新增一条导出记录。

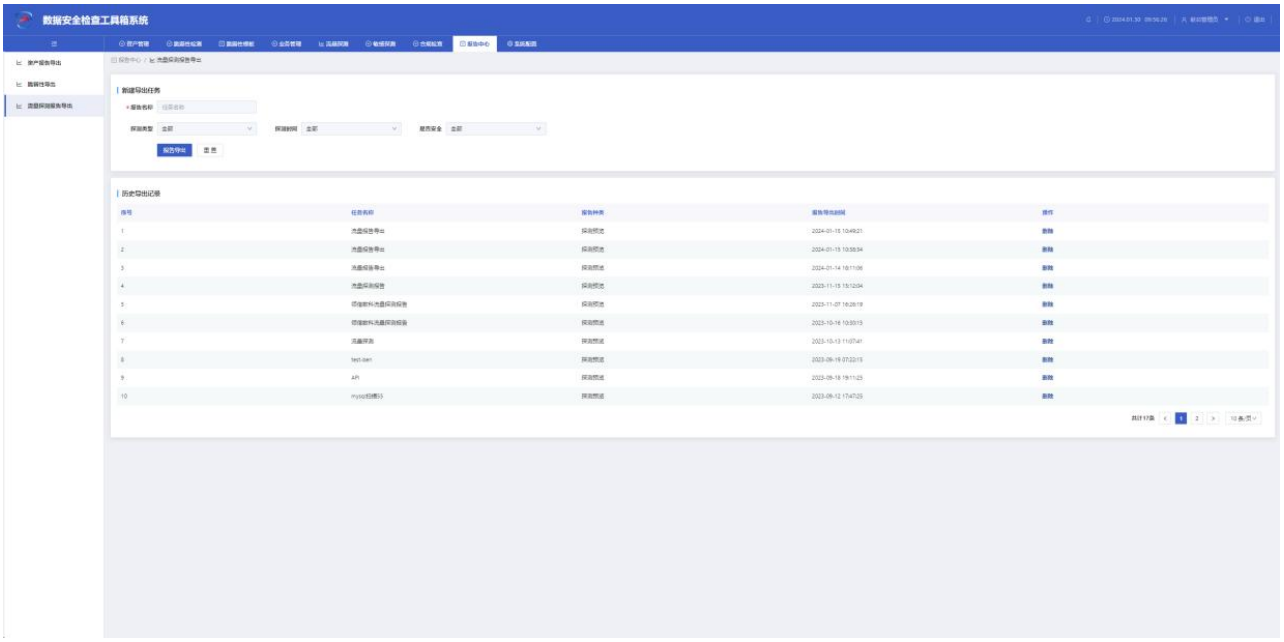


图 9.3 流量探测报告导出

十. 系统配置

系统配置目前当前只有系统监控页面。

10.1 系统状态

系统状态页面，展示设备信息、运行状态、CPU/内存/交换分区使用率、版本号等信息。

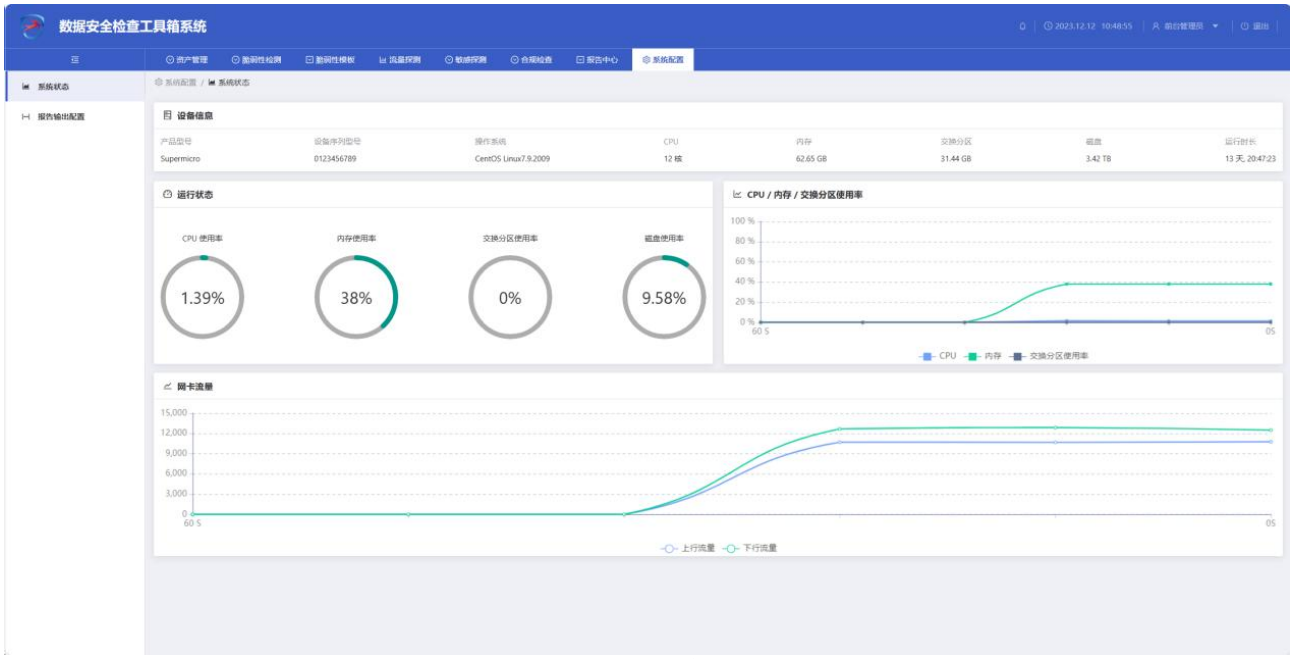


图 10.1 系统状态

10.2 报告输出配置

KAFKA 输出：可以配置 KAFKA 地址，将部分数据推送过去。

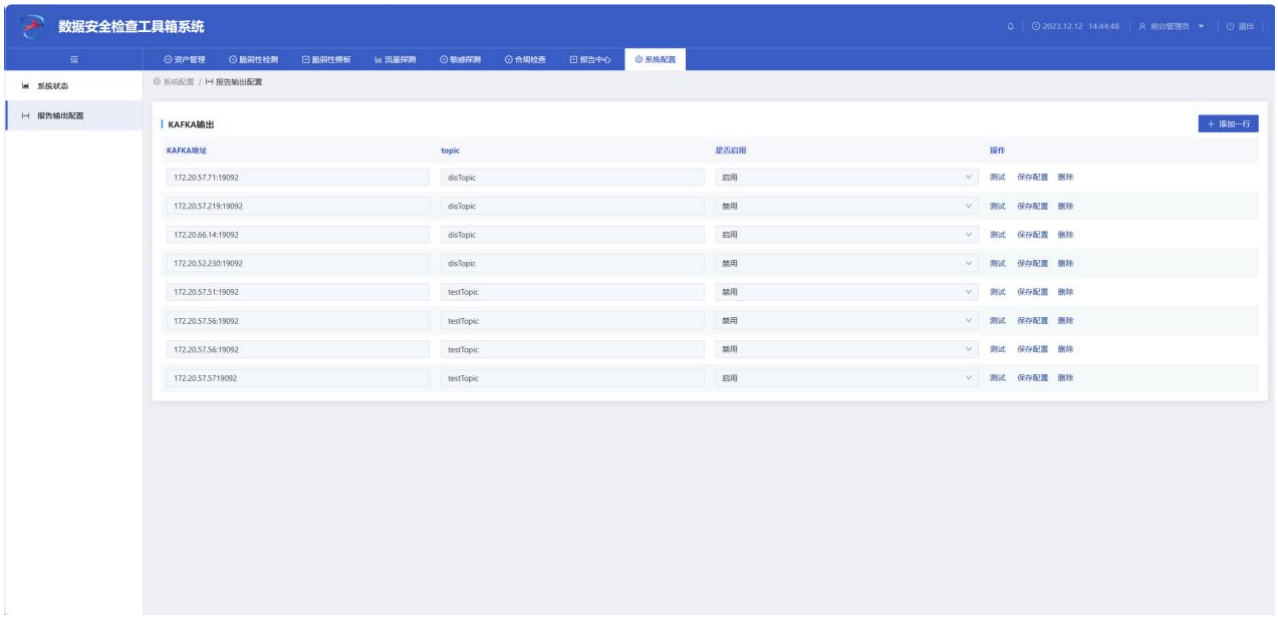


图 10.2 系统监控

操作：在报告输出配置页面，点击【添加一行】，自动创建后输入 KAFKA 地址、topic、是否启用。

10.3 出境填报

WEBUI：主界面 -> 系统配置 ->出境填报

出境填报功能，旨在于解决例如网信办等场景下的出境分析问题。新增的出境数据，根据出境源 IP、出境目的 IP、出境数据白名单、传输条数匹配，敏感数据在条件范围内属于白名单，可不命中响应的敏感数据模型，超出条数范围/出境数据白名单范围，可在探测告警中命中出境账实不符模型。

图 10.3 出境填报列表

图 10.2 新增填报

操作：在填报列表页面，点击“新增填报”按钮，输入被检单位、出境源 IP、出境目的 IP、出境填报人、出境白名单、传输条数、业务概述等信息，点击“确认”。

新增成功会在页面生成对应的填报记录。

10.4 诊断工具

10.4.1 端口探测工具

WEBUI：主界面 -> 系统配置 -> 诊断工具-> 端口探测工具

进入端口探测工具页面，输入探测 IP/域名，探测端口/范围，点击“探测”，可进行 IP

及端口范围的探测。

图 10.4.1 端口探测工具

10.4.2 Ping 工具

WEBUI：主界面 -> 系统配置 -> 诊断工具-> ping 工具

进入 ping 工具页面，输入对应的资产 ip 或域名，点击“测试”，可进行目标资产的网络扫描检测。

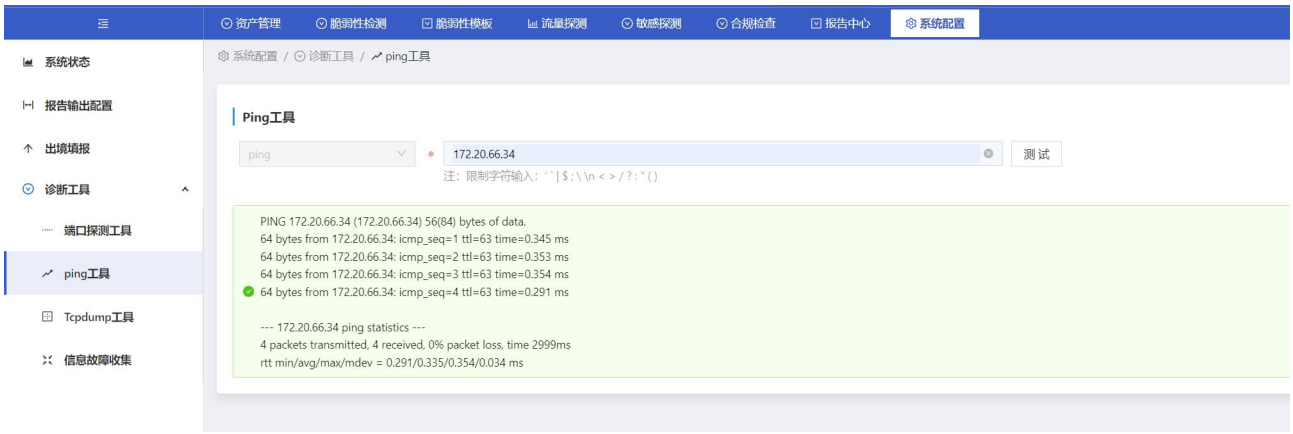


图 10.4.2 ping 工具

10.4.3 Tcpdump 工具

WEBUI：主界面 -> 系统配置 -> 诊断工具-> Tcpdump 工具

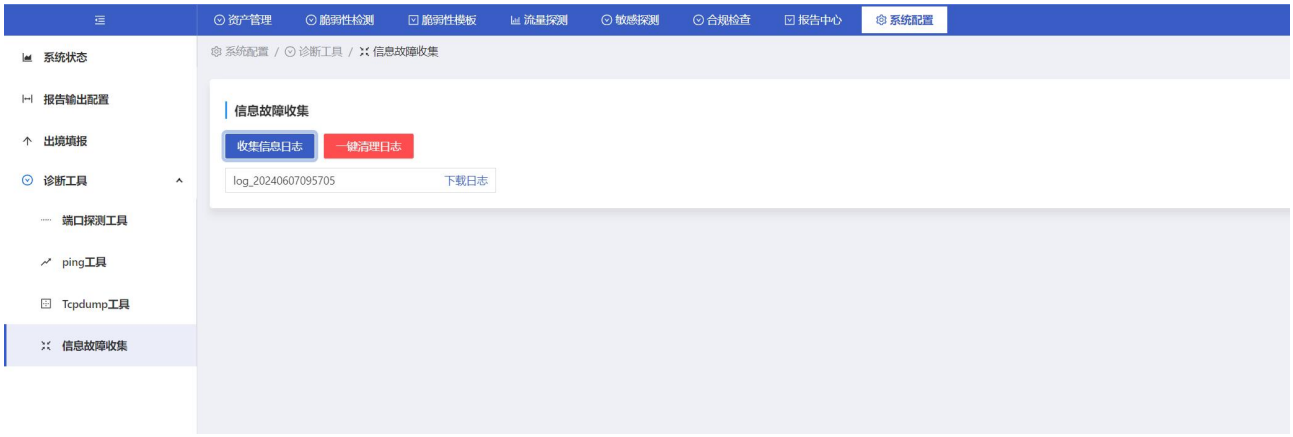
进入 tcpdump 工具页面，选择协议类型、输入相应的数据条目、接口、主机 IP/域名，点击启动，停止后可下载相应的抓包文件。

图 10.4.3 Tcpdump 工具

10.4.4 信息故障收集

WEBUI：主界面 -> 系统配置 -> 诊断工具-> 信息故障收集

进入信息故障收集页面，点击“收集日志信息”，可进行 bld、as_bin 的日志信息收集。点击“一键清理日志”，可清除页面当前数据显示及后台服务器上存储的日志文件。



10.4.4 信息故障收集

十一. Sysadmin 系统配置

Sysadmin 账户登录访问系统配置页面。

11.1 系统状态

系统状态页面，展示设备信息、运行状态、CPU/内存/交换分区使用率、版本号等信息。

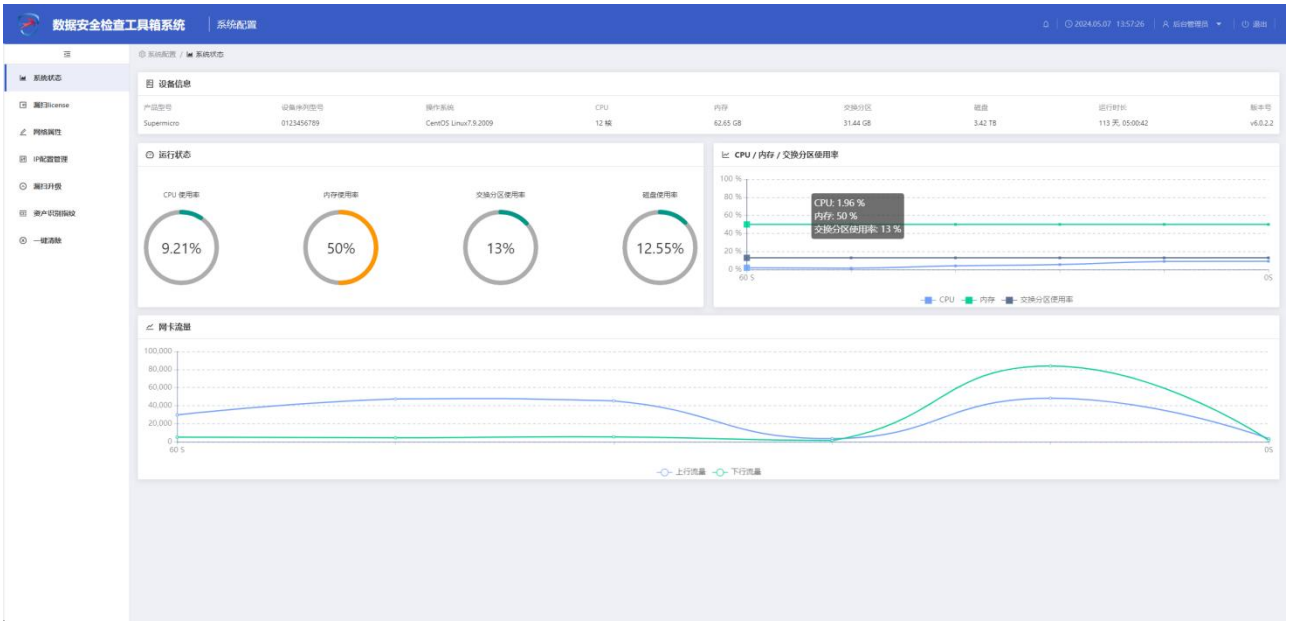


图 11.1 系统状态

11.2 漏扫 license

漏扫 license：可进行漏扫功能的 license 授权操作。

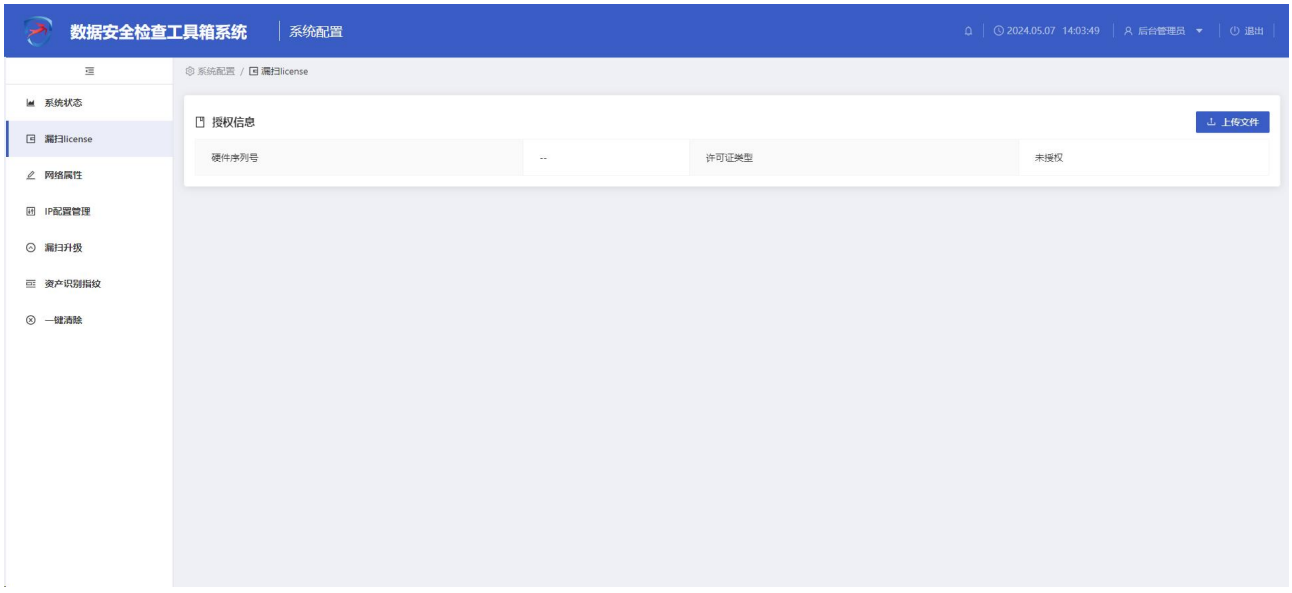


图 11.2-1 漏扫 license

操作：在漏扫 license 页面，点击【上传文件】，选择对应的.dat 文件进行上传，授权后的页面如图所示。

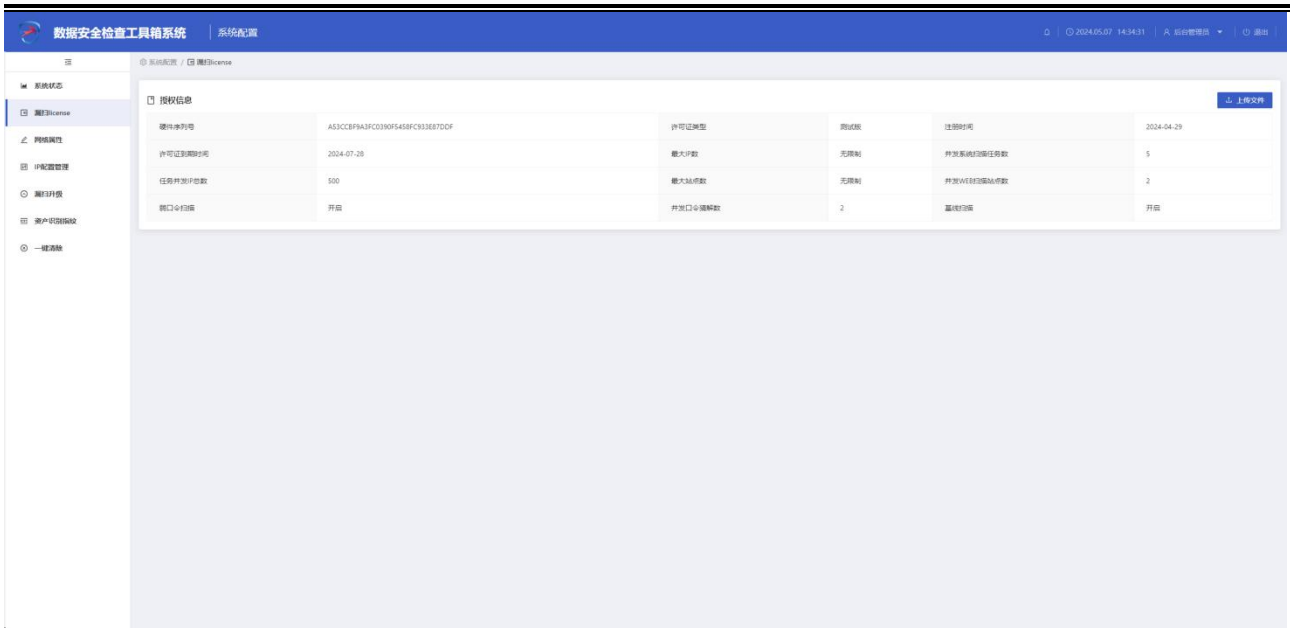


图 11.2-2 授权后漏扫 license

11.3 网络属性

网络属性：网络属性页面可查看网卡相关信息，可进行网络地址、掩码、网关的配置等操作。

操作：选择对应的网卡，PING 控制选择“允许”/“禁止”，修改地址与掩码，网关的配置信息，点击“保存”，可成功进行网卡信息的修改。

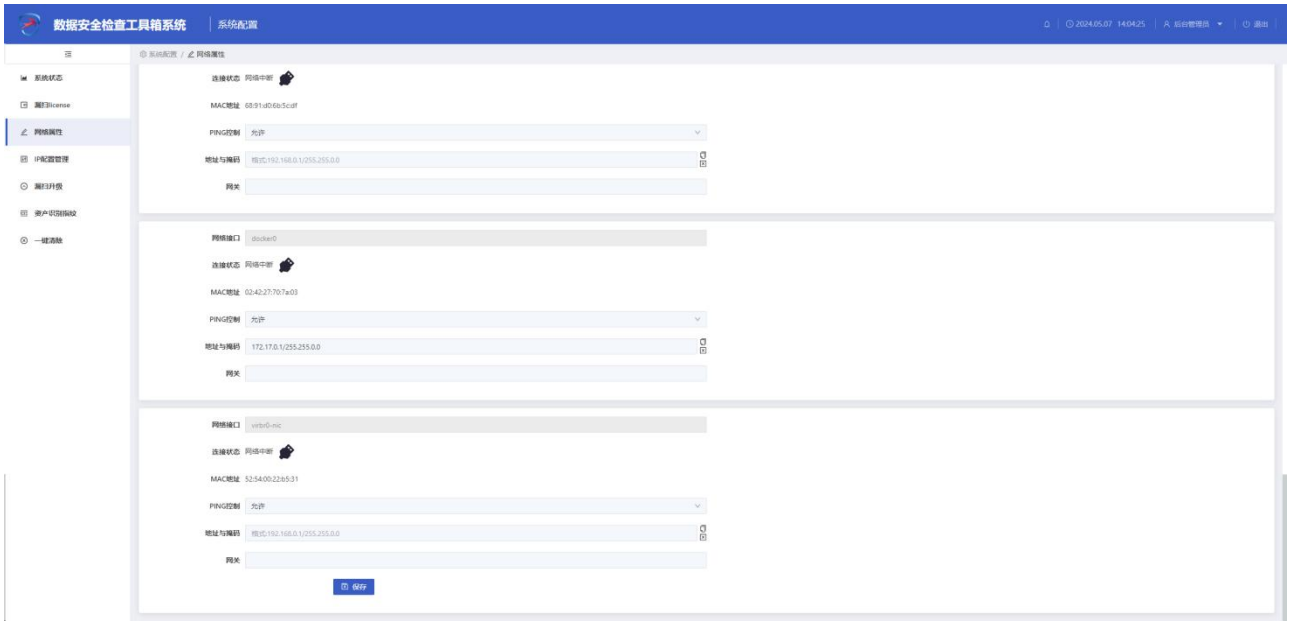


图 11.3 网络属性

11.4 IP 配置管理

IP 配置管理：可以进行 kafka IP 或端口信息的配置，也可以进行探针的 IP、端口、镜像网口的配置。

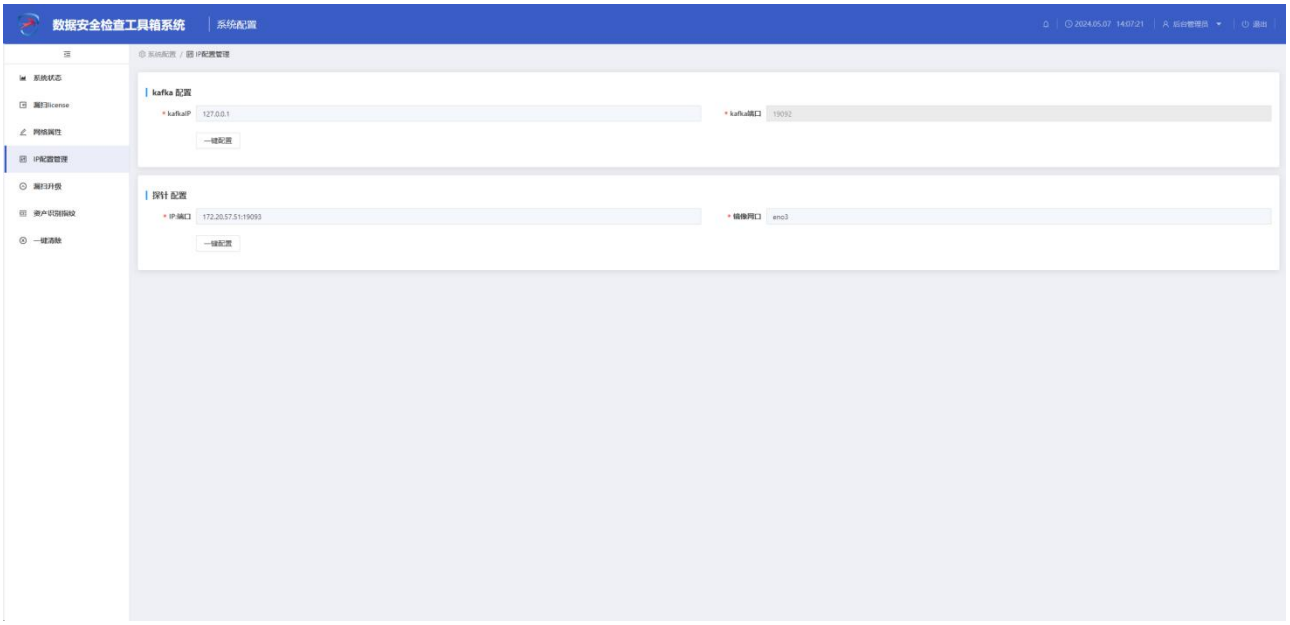


图 11.4 IP 配置管理

操作：在 IP 配置管理页面，输入 kafkaIP、kafka 端口信息，点击“一键配置”；输入探针的 IP:端口、镜像网口信息，点击“一键配置”，分别进行系统自身 kafka 和探针的信息配置，如图所示。

11.5 漏扫升级

漏扫升级：可以进行漏扫功能的规则库在线升级、系统/规则库/补丁 FTP 升级、系统/规则库/补丁离线升级操作。

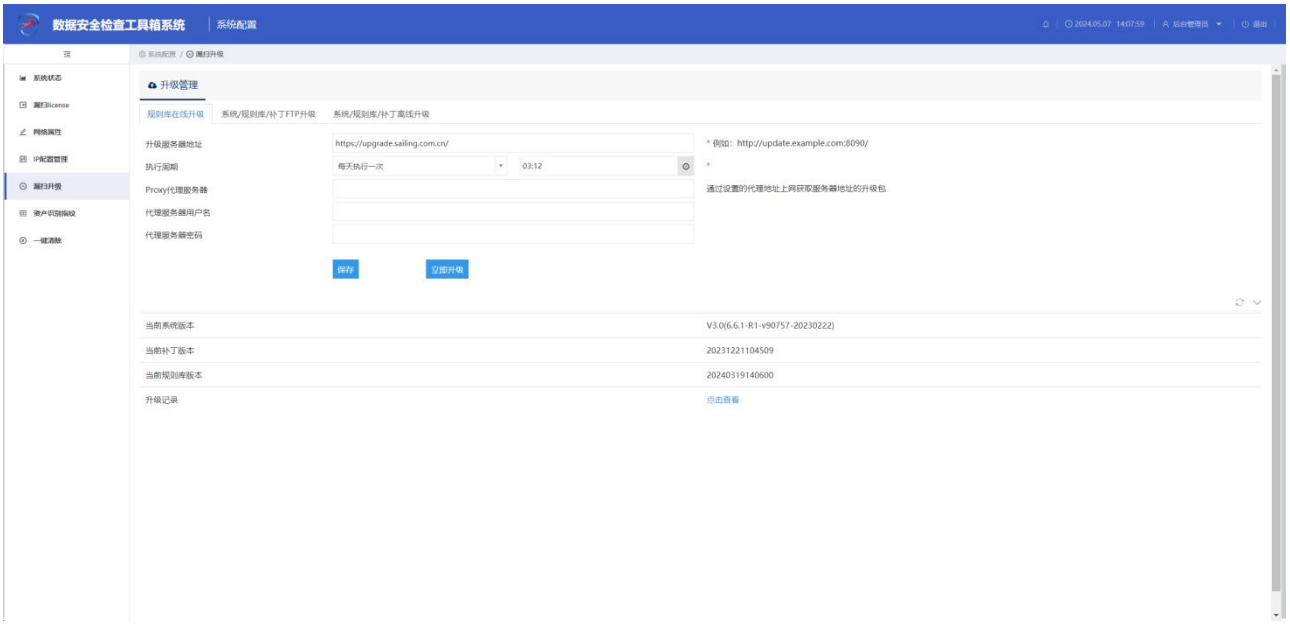


图 11.5 漏扫升级

操作：准备相应的在线规则库或离线规则库，在漏扫升级页面配置相关的代理服务器信

息或上传本地的离线升级包，点击“升级”，进行漏扫规则库的升级，如图所示。

11.6 资产识别指纹

资产识别指纹：进行边界链路的配置，并在资产扫描的结果中匹配对应的资产识别指纹。

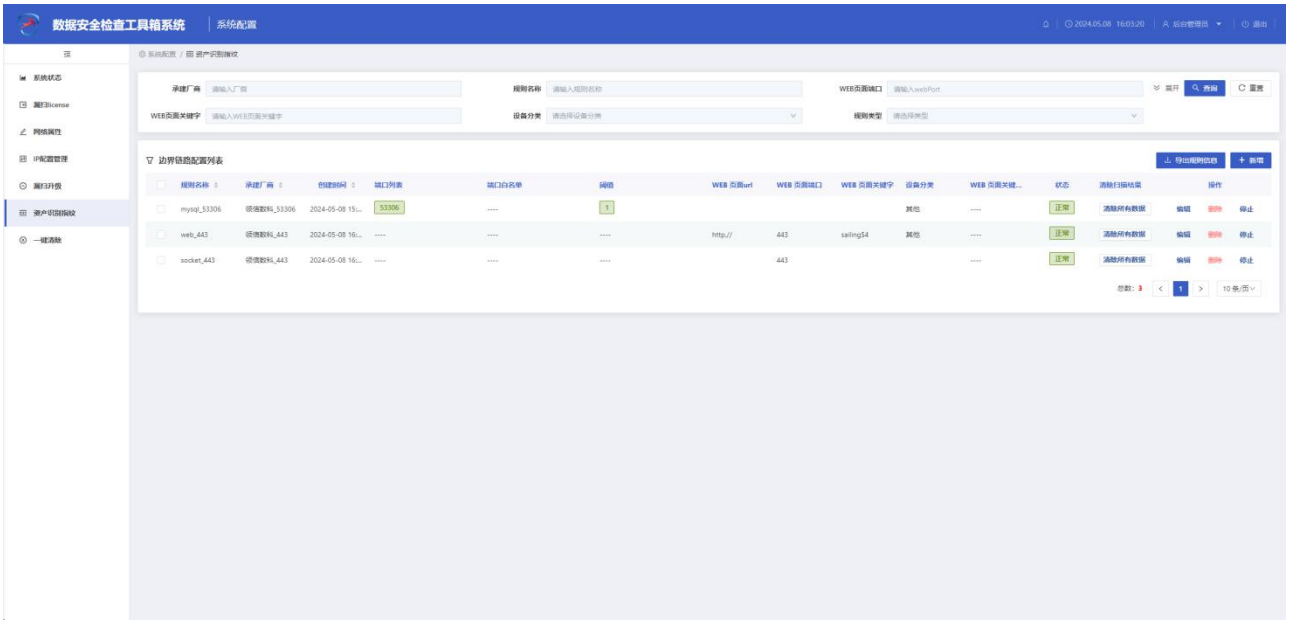


图 11.6-1 资产识别指纹

操作：在资产识别指纹页面，点击“新增”，如图所示，分别填写端口配置、WEB 页面配置、socket 配置，点击“保存”。

图 11.6-2 新增边界链路配置

dcbox 账户登录系统，在资产扫描页面查看配置生效结果。

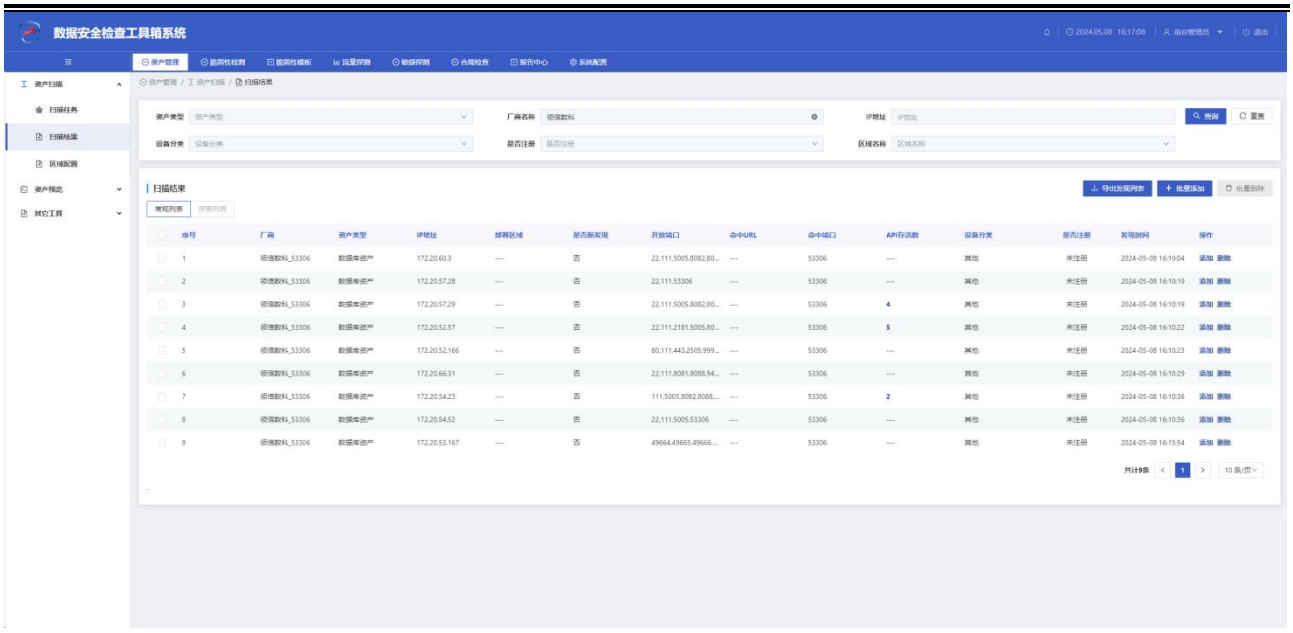


图 11.6-3 资产识别指纹生效

11.7 一键清除

一键清除：分模块进行数据清除，并记录清除记录。

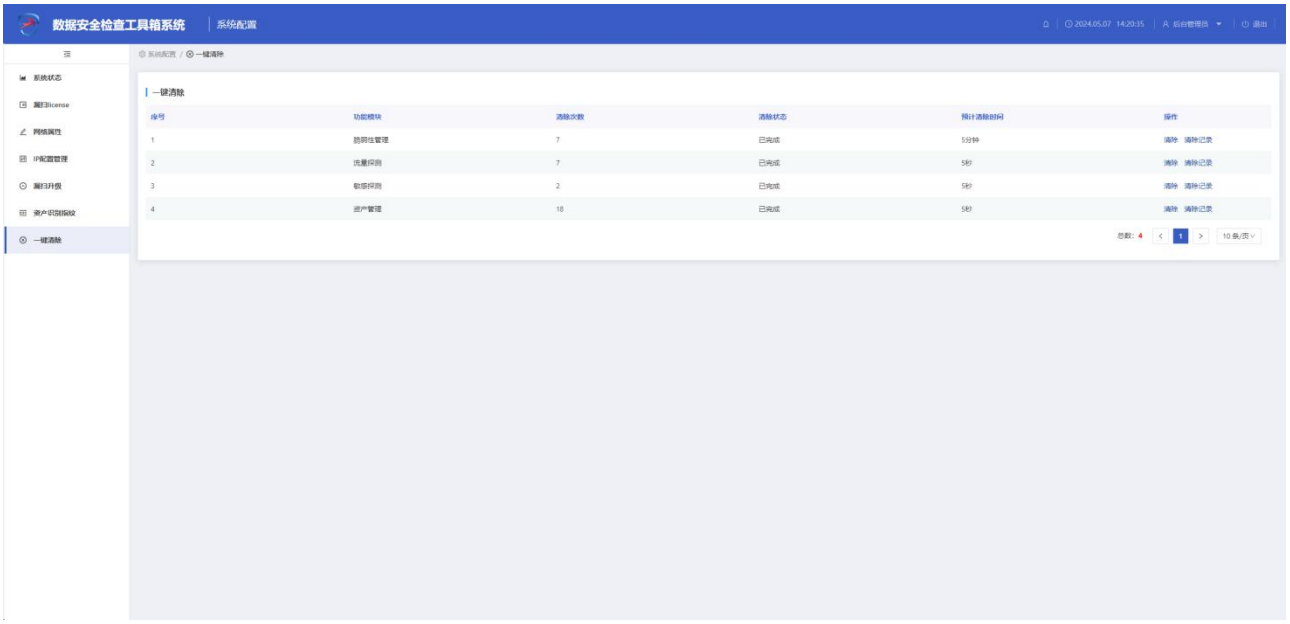


图 11.7-1 一键清除

操作：在一键清除页面，选择对应的模块，点击“清除”按钮，在弹出的二次确认框中点击“确定”。相关模块的数据会被清除。

脆弱性管理：清除脆弱性检测-任务管理、脆弱性资产、脆弱性资产组，脆弱性模板-基线策略模板，报告中心-脆弱性导出；影响资产管理-资产预览-风险资产管理的数据评分；

流量探测：清除流量探测-新建任务、探测预览，报告中心-流量报告、综合报告内容；影响资产管理-资产预览-风险资产管理的数据评分；

敏感探测：清除敏感探测-敏感数据发现内容；

资产管理：清除资产扫描-扫描任务、扫描结果、区域配置，资产预览-资产台账、资产测绘、风险资产管理，敏感探测-数据库资产，报告中心-资产台账、综合报告内容。

点击“清除记录”，可查看对应模块的清除记录。

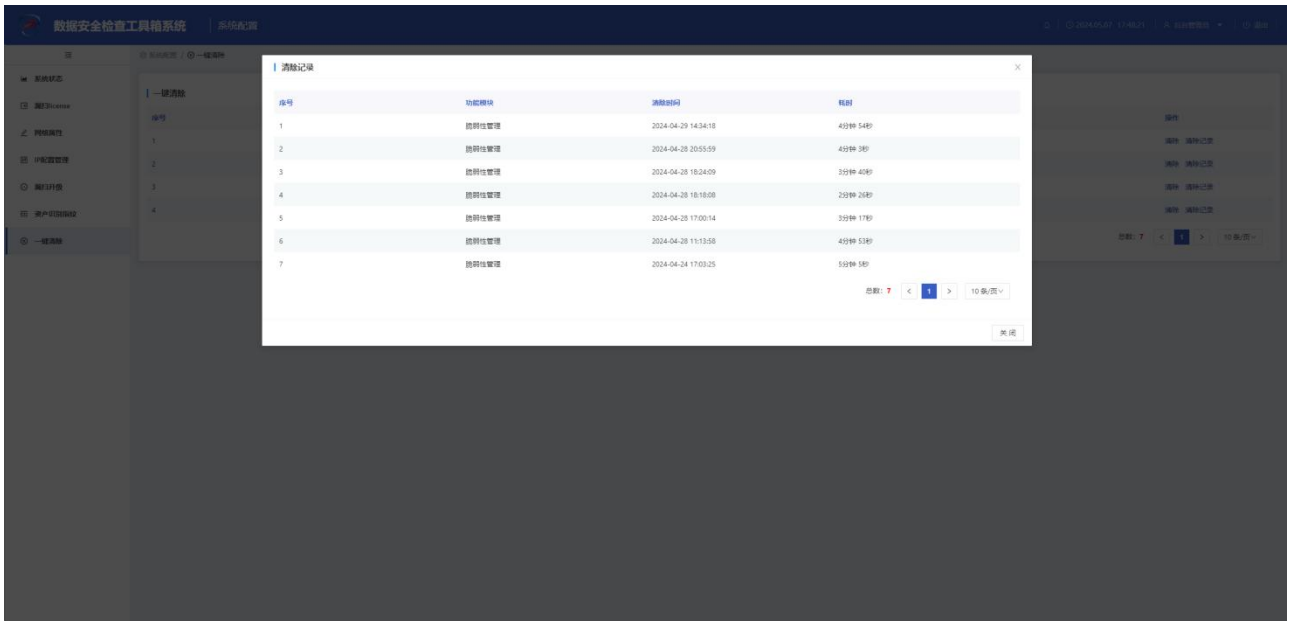


图 11.7-2 清除记录