UNIS X1000-12T12F-G2 紫光漏洞扫描系统

用户手册

目录

前言

概述

本文将对紫光漏洞扫描系统（UNIS X1000-12T12F-G2）的所有功能点详细介绍它的主要功能模块和使用方法。

读者对象

本文档主要适用于以下读者：

- 系统管理员
- 网络管理员

1 产品概述

UNIS X1000-12T12F-G2 是紫光恒越自主研发的新一代漏洞发现管理系统，涵盖了资产管理、风险管理、系统扫描、应用扫描、应用监控、数据库扫描、基线配置核查、口令猜解、移动应用扫描、镜像漏洞扫描、报表管理、辅助工具、日志管理、系统管理等模块，本章将介绍与 UNIS X1000-12T12F-G2 相关的基础知识。

1.1 产品特点

1.1.1 领先、丰富的漏洞知识库

系统漏洞知识库的检测脚本大于 300000 条，涵盖了各种主流操作系统、应用服务、网络设备、数据库、工控系统、大数据组件、虚拟化平台系统等。漏洞知识库数量国内领先。漏洞相关信息支持全中文，兼容 CVE 等标准，漏洞修复建议清晰、详细，可操作性强。

1.1.2 全面、统一的漏洞扫描

UNIS X1000-12T12F-G2 集成了系统扫描、应用扫描、应用监控、数据库扫描、基线配置核查、镜像漏洞扫描、移动 APP 扫描、口令猜解七大扫描模块，能够全面发现信息系统存在的各种脆弱性问题，包括各类安全漏洞、安全配置问题、不合规行为、弱口令以及不必要开放的端口等，形成整体安全风险报告，一目了然。

1.2 典型部署

UNIS X1000-12T12F-G2 是根据网络 IP 地址分布情况进行配置的，它可以部署在网络的任何地方，只要能够访问到要进行安全评估的目标系统就能够正常工作。

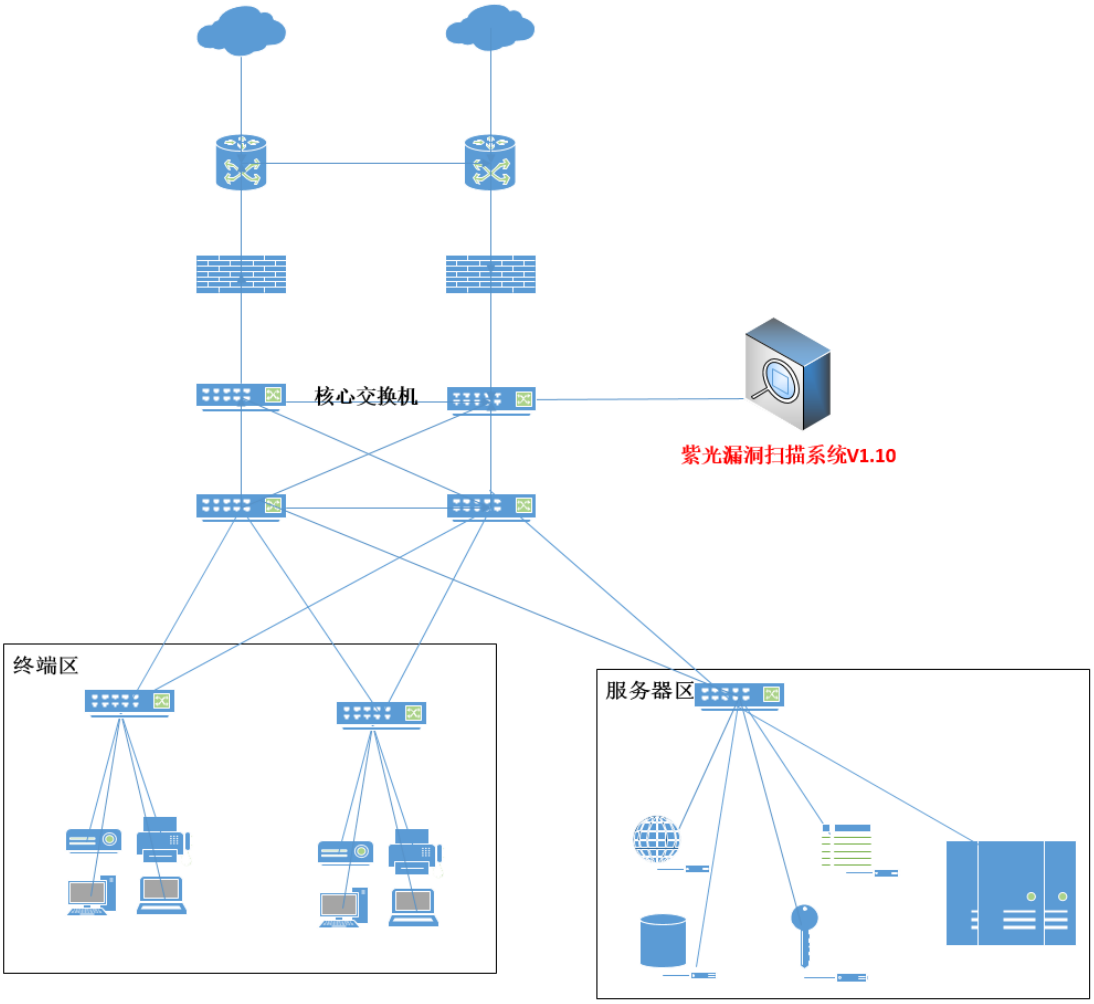


图 1-1 部署拓扑图

1.3 使用流程

UNIS X1000-12T12F-G2 风险管理流程如图所示：

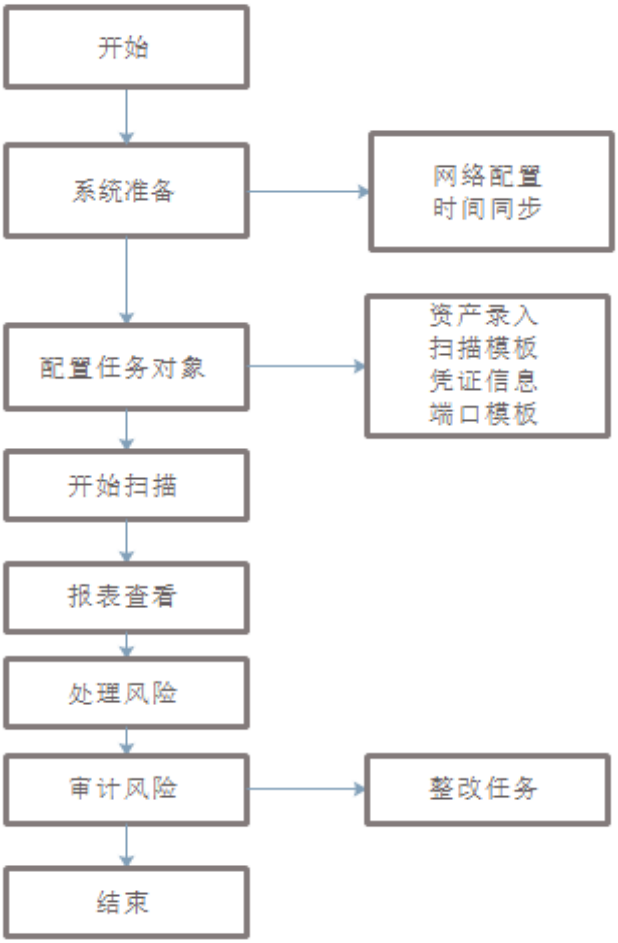


图 1-2 风险管理流程

2 登陆管理

本章主要介绍 UNIS X1000-12T12F-G2 的两种登陆方式。

2.1 Web 登陆管理

Web 管理系统为管理员提供了更直观的人机交互方式，管理员通过 Web 管理界面实现对 UNIS X1000-12T12F-G2 的管理和配置。

2.1.1 Web 用户

系统用户采用三权分立设计原则，分为管理员、审计员和安全员，用户信息如下：

角色	初始账号/密码	权限说明
管理员	admin/admin@ZGhy2024	可以进行系统设置、用户设置等
安全员	user/user@ZGhy2024	扫描功能模块使用
审计员	audit/audit@ZGhy2024	日志审计查询
超级管理员	superadmin/superadmin@ZGhy2024	拥有所有权限

2.1.2 Web 登陆

本节以 Chrome 浏览器为例，介绍登录 UNIS X1000-12T12F-G2 的 Web 管理系统的详细步骤。

（一） 使用网线连接设备的管理口，管理口默认 IP 地址为 192.168.0.200，计算机 IP 需要与管理口在同一网段。

（二） 登陆 Web 管理界面

（三）

a. 打开浏览器，用 HTTPS 方式连接 UNIS X1000-12T12F-G2 的管理口 IP。例：https://192.168.0.200。弹出安全报警信息，如图所示：

图 2-1 提示信息

选择继续前往此站点

b. 在弹出的 Web 登录界面中，输入系统管理员的用户名和密码，如图所示。

图 2-2 系统登陆框

如果系统管理员 admin 的登录密码丢失，可以在控制台中进行恢复，具体操作方法请参见 2.2.3 控制台说明。

（四）配置网络信息

a. 进入【系统管理】-【设备管理】中“网络管理”，进入网络配置界面，如下所示：

★注意：

1. 系统第一次登陆，需要强制修改用户的初始密码。

图 2-3 网络配置列表

b. 单击操作栏中的编辑，在弹出对话框中配置扫描口 IP 地址、子网掩码、网关、DNS 等参数，如图所示：

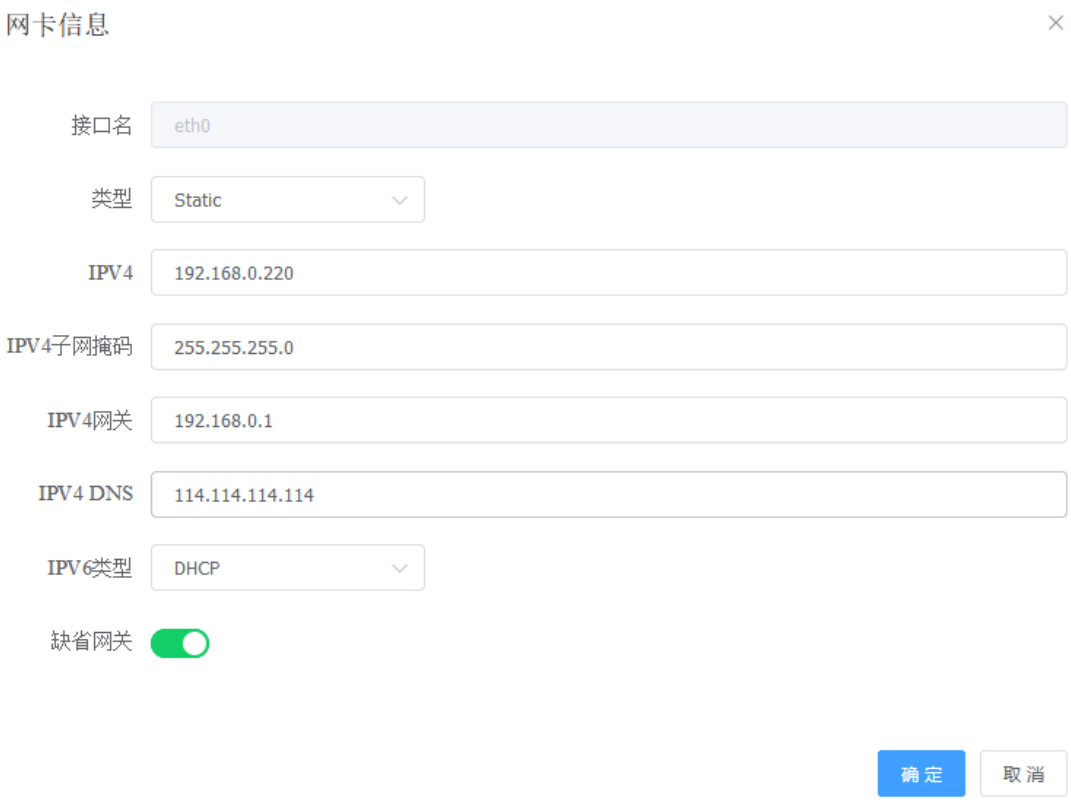


图 2-3 网卡配置

c. 将上面配置的 UNIS X1000-12T12F-G2 的网口接入网络。打开浏览器，用 HTTPS 方式连接网口 IP。可正式投入使用，进行对目标网络的安全评估。

2.1.3 Web 页面布局

user 用户成功登录，进入 Web 系统管理界面，页面布局如图所示：

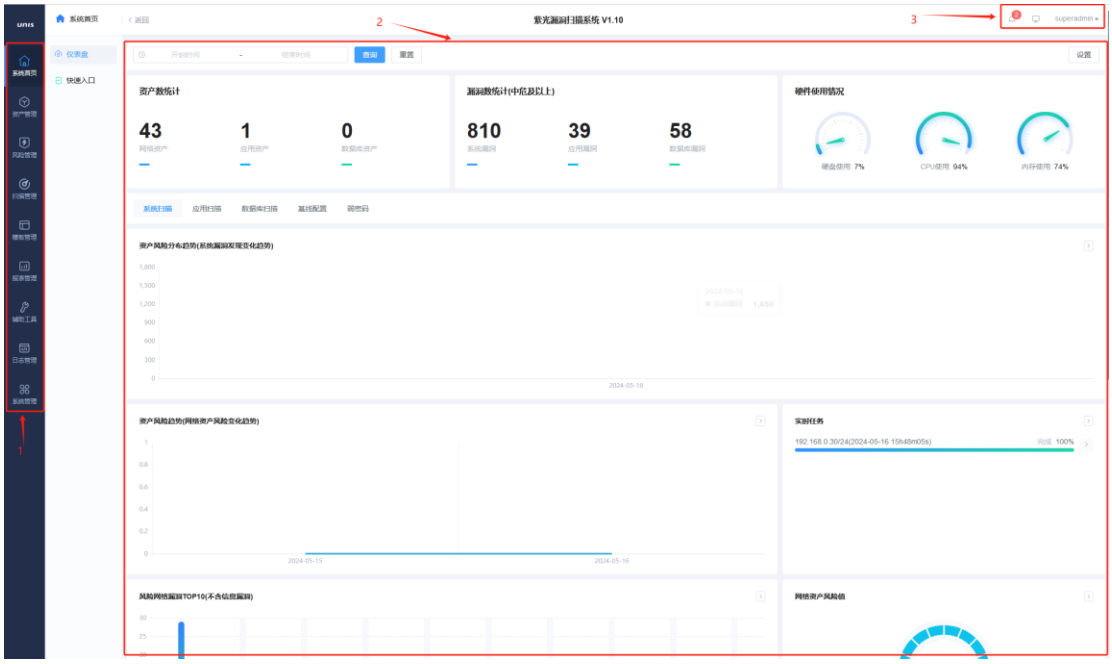


图 2-5 系统首页

1、导航树	系统的路径导航栏。
2、快捷操作栏	系统设定的几个快捷按键，按键的详细功能如下。 • ：风险态势分析大屏展示。 • ：系统通知。 superadmin：当前用户
3、工作区	系统扫描资产信息、风险情况、系统状态监控信息、任务查看等。(支持客户化定制仪表盘功能，具备多种仪表盘模版，用户可根据需求，完全自定义仪表盘显示)

表 2-1 页面布局说明

2.2 控制台管理

通过串口或者 SSH 远程访问连接可以访问 UNIS X1000-12T12F-G2 的控制台管理界面，管理员可以对 UNIS X1000-12T12F-G2 进行系统初始配置、恢复初始化配置等功能，某些 Web 管理界面中无法进行管理的部分，可以在此进行管理操作。

2.2.1 控制台用户

连接方式	用户名/密码	备注
SSH	console/unisPassw0rd	端口：22
串口	console/unisPassw0rd	波特率：9600

表 2-2 控制台登陆用户说明

2.2.2 控制台登陆

（一）控制台主菜单，控制台界面如下图：

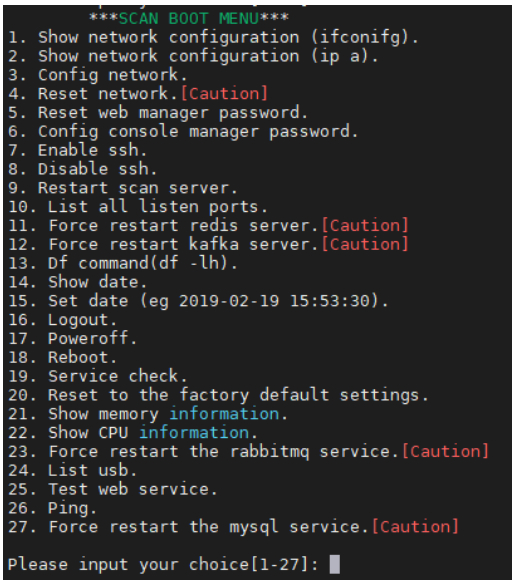


图 2-6 控制台选项

（二）控制台配置网卡信息

a. 输入序号“3“，回车；然后选择网卡，输入网卡序号，回车。以 eth0 网卡为例：

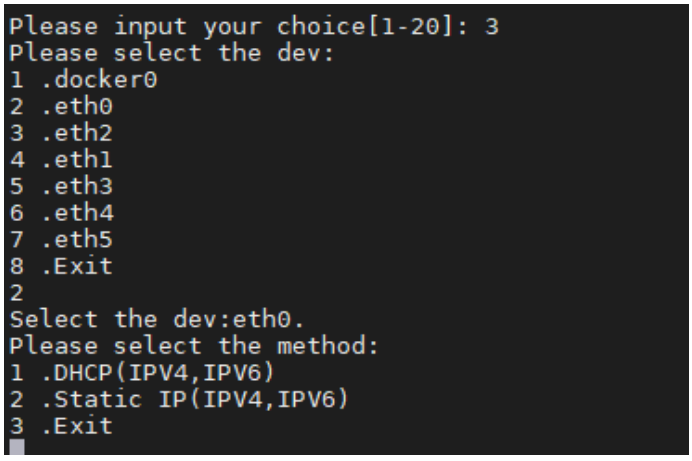


图 2-6 控制台网卡配置

b. 选择网络 IP 获取方式，输入对应的序号进行配置。

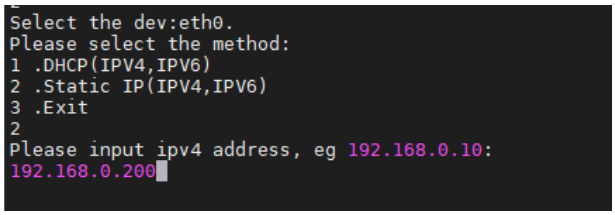


图 2-7 控制台网卡配置

2.2.3 控制台说明

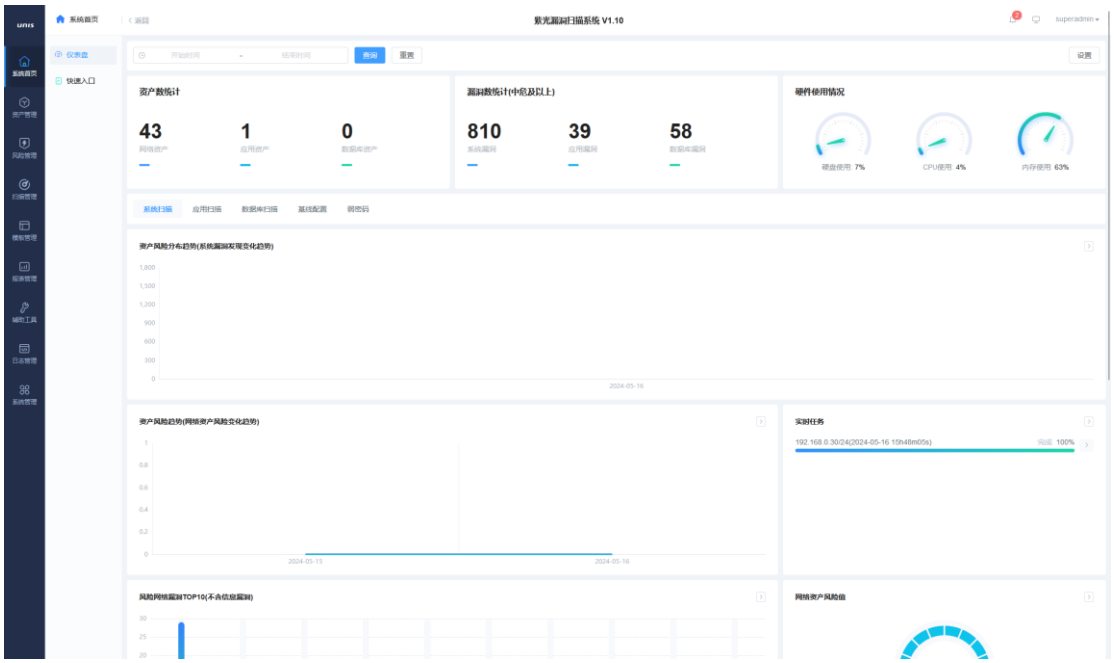
序号	名称	说明
1	Show network configuration (ifconfig)	查看服务器网络信息
2	Show network configuration (ip a)	查看服务区 IP 信息
3	Config network	配置网卡 IP 地址
4	Reset network.	重置网络配置
5	Reset web manager password	重置初始用户密码
6	Config console manager password	修改服务器 console 账户密码
7	Enable ssh.	设置 SSH 服务开机自启
8	Disable ssh	设置禁用 SSH 服务自启
9	Restart scan server.	重启应用服务
10	List all listen ports.	查看监听端口
11	Restart redis server	重启 redis 服务（谨慎操作）
12	Force restart kafka server.	重启 kafka 服务（谨慎操作）
13	Df command(df -lh)	查看服务器分区信息
14	Show date	查看系统时间
15	Set date (eg 2019-02-19 15:53:30)	配置系统时间
16	Logout	退出系统当前账号

17	Poweroff	关机
18	Reboot	重启
19	Service check	查看应用服务状态
20	Reset to the factory default settings	清空系统数据库
21	Show memory information.	显示设备内存使用信息
22	Show CPU information.	显示设备 CPU 使用信息
23	Force restart the rabbitmq service.	强制重启消息队列（在厂商指导下操作）
24	List usb.	显示设备 USB 口接入信息
25	Test web service.	检测 web 服务运行情况
26	Ping	Ping 测试
27	Force restart the mysql service	重启 mysql 服务

表 2-2 控制台选项说明

3 系统首页

首页展示检查网络资产数、网络漏洞数（中危及以上）、网络扫描任务总数、网络扫描执行任务总数、系统 CPU、内存、硬盘使用情况、支持客户化定制仪表盘功能，具备多种仪表盘模版，用户可根据需求，完全自定义仪表盘显示;图表展示网络漏洞风险等级分布、图表展示操作系统分布、图表展示端口暴露面分布、网络风险漏洞 TOP10、风险网络资产 TOP10 等分析展示等以及态势风险可视化大屏以及扫描任务的快速入口。



3.1 仪表盘展示

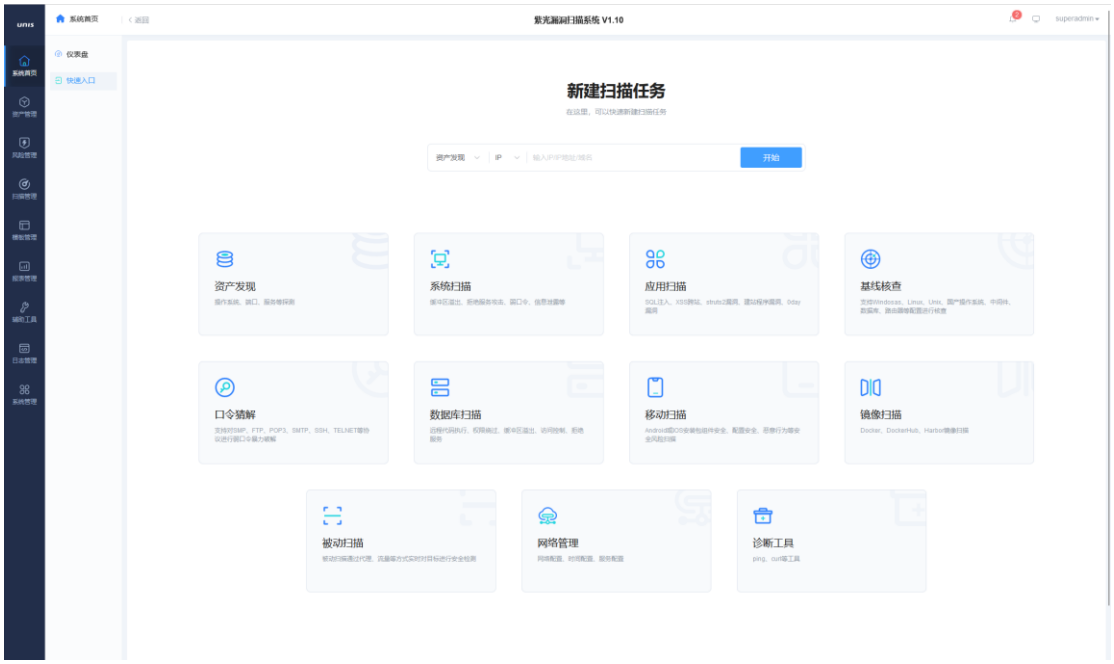
仪表盘展示的内容如下表

统计项	描述
开始时间~结束时间	设置要展示任务信息和分析图表的任务时间段，为空则表示当前时间前的所有任务数据
查询	点击根据设定的时间段进行展示
设置	设置首页图表展示的内容，可设置图表显示/隐藏、图表展示样式等

网络资产数	资产管理中的网络资产的总数量
系统漏洞数（中危及以上）	风险检测中系统扫描任务里所有任务的扫描结果中，包含危险等级为中危及以上的漏洞数量
应用资产数	资产管理中的应用资产的总数量
应用漏洞数（中危及以上）	风险检测中应用扫描任务里所有任务的扫描结果中，包含危险等级为中危及以上的漏洞数量
数据库资产数	资产管理中的数据库资产的总数量
数据库资产漏洞数（中危及以上）	风险检测中数据库扫描任务里所有任务的扫描结果中，包含危险等级为中危及以上的漏洞数量
系统漏洞新增变化趋势	折线图展示系统漏洞数的新增变化趋势
应用漏洞发现变化趋势	折线图展示应用漏洞数的新增变化趋势
系统漏洞等级风险分布	所有主机扫描结果的风险等级占比情况
应用漏洞等级风险分布	所有应用扫描结果的风险等级占比情况
数据库漏洞等级风险分布	所有数据库扫描结果的风险等级占比情况
操作系统分布	网络资产中的操作系统分布占比情况
端口暴漏面分布	系统扫描任务中发现的资产端口暴漏面 TOP10 分布比例
网络风险漏洞 TOP10(不含信息漏洞)	系统扫描任务中发现的漏洞 TOP10
应用风险漏洞 TOP10(不含信息漏洞)	应用扫描任务中发现的漏洞 TOP10
数据库风险漏洞 TOP10(不含信息漏洞)	数据库扫描任务中发现的漏洞 TOP10
风险网络资产 TOP10(不含信息漏洞)	网络资产中风险漏洞数 TOP10 分析展示
风险应用资产 TOP10(不含信息漏洞)	应用资产中风险漏洞数 TOP10 分析展示
风险数据库资产 TOP10(不含信息漏洞)	数据库资产中风险漏洞数 TOP10 分析展示
基线配置核查不符合项 TOP10	基线配置核查任务结果不符合项 TOP 展示
基线配置核查不符合 IP TOP10	基线配置核查目标不符合项 TOP10 展示
弱密码分布 TOP10	口令猜解结果弱密码分布 TOP10 展示
弱密码 IP 分布 TOP10	口令猜解结果弱密码 IP TOP10 展示

3.2 快速入口

快速入口页面方便用户快捷发起扫描任务，包括资产发现任务、系统扫描任务、应用扫描任务、数据库扫描任务、基线核查任务、口令猜解任务、移动扫描任务、应用监控任务、镜像扫描任务、网络配置、诊断工具快速使用等。



快速入口内容如下表所示：

名称	描述
资产发现	快速发起 IP 资产存活发现任务和子域名猜解任务
应用扫描	快速发起 web 应用漏洞扫描任务
系统扫描	快速发起系统漏洞扫描任务
基线核查	快速发起基线配置检测任务
弱口令扫描	快速发起弱口令扫描任务
应用监控	快速发起 web 网站监控任务
数据库扫描	快速发起数据库漏洞扫描任务
移动扫描	快速发起移动 APP 检测任务
镜像扫描	快速发起镜像漏洞扫描任务
被动扫描	快速发起 web 网站被动方式的漏洞扫描任务
网络管理	快速进入系统的网络配置管理页面
诊断工具	快速进入诊断工具使用页面

3.3 资产风险态势感知大屏

点击系统首页右上方 图标，进入风险态势可视化大屏展示页面。

大屏展示内容参数说明

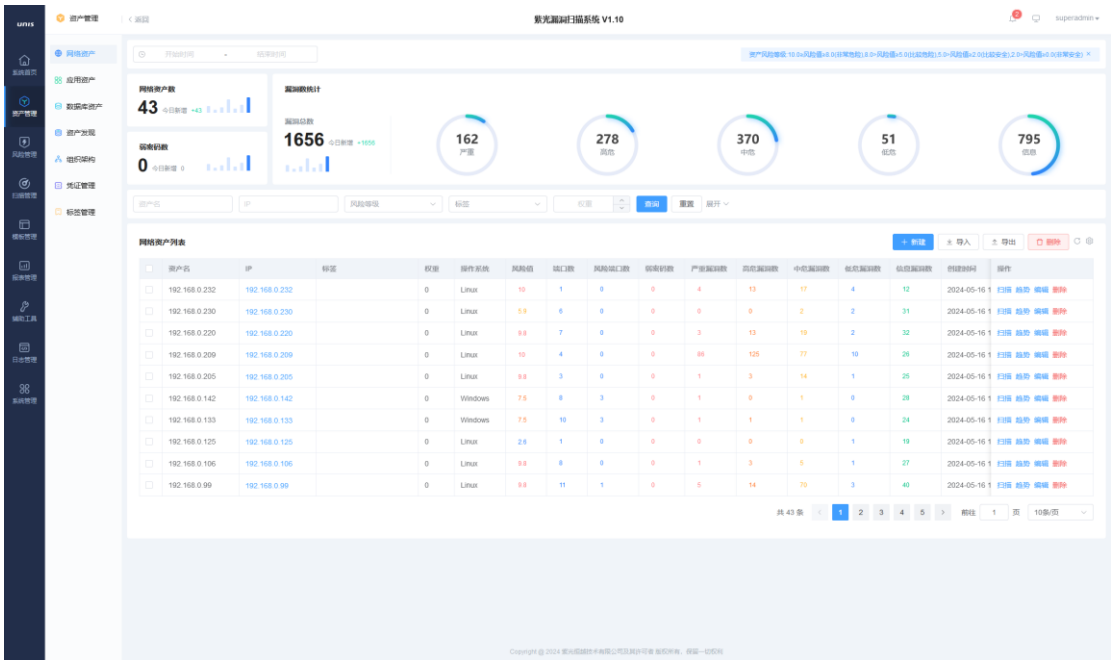
显示项	描述
网络资产	网络资产库的资产总数
应用资产	应用资产库的资产总数
数据库资产	数据库资产库的资产总数
系统漏洞数	系统扫描结果的漏洞总数（中危及以上）
应用漏洞数	应用扫描结果的漏洞总数（中危及以上）
数据库漏洞数	数据库扫描结果漏洞总数
端口暴露面分布	系统扫描结果的暴露端口分布情况
风险网络资产 TOP5	网络资产库中风险网络资产 TOP5 展示
风险应用资产 TOP5	网络资产库中风险应用资产 TOP5 展示
风险数据库资产 TOP10	网络资产库中风险数据库资产 TOP10 展示
数据库漏洞等级分布	数据库扫结果统计漏洞等级的分布占比
应用漏洞 TOP10	应用扫描结果中漏洞出现情况 TOP10(不含信息漏洞)

4 资产管理

系统综合运用多种手段，全面、快速、准确的发现被扫描网络中的存活主机，准确识别其属性，包括主机名称、IP 地址、端口、操作系统、软件版本、负责人、地区等，为进一步漏洞扫描做好准备，同时资产列表可以展示操作系统、端口数、严重漏洞数、高危漏洞数、中危漏洞数等信息。

4.1 网络资产

网络资产主要用于网络内主机/应用资产的管理，查看全网主机资产的风险脆弱情况，网络资产页面可以添加、导入管理网络中的主机资产，页面如下：



资产管理内容参数说明

显示项	描述
资产名	输入要查找的资产名称
ip	输入要查找的资产 IP

	风险等级根据资产风险值计算，可以进行风险等级筛选
	选择资产标签进行筛选
	展示设置的权重值资产
	选择资产的主机/应用类型进行筛选
	选择资产的配置规范进行筛选
	输入资产的负责人信息进行筛选
	输入联系方式进行筛选
	输入邮箱进行筛选
	点击进行搜索
	点击清空筛选条件
	新建网络资产
	导入网络资产
	导出所有网络资产，格式为 xlsx
	删除列表中选中的网络资产

资产列表内容参数说明

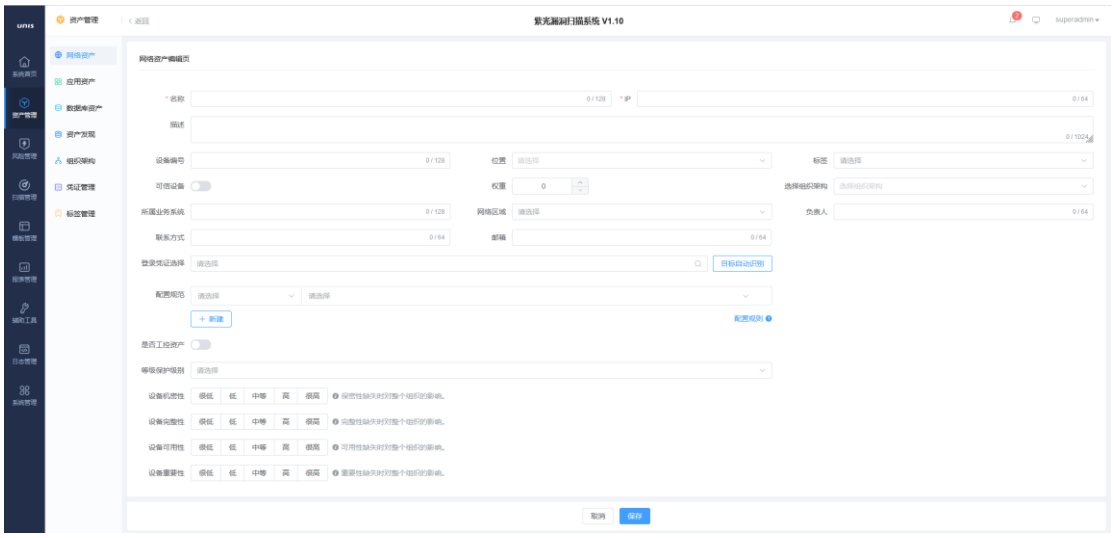
显示项	描述
资产名	此网络资产的资产名称
IP	此网络资产的 IP 地址信息
标签	资产标签信息
操作系统	资产操作系统信息
权重	资产权重值
风险值	资产风险值（资产风险等级:10.0≥风险值≥8.0(非常危险),8.0>风险值≥5.0(比较危险),5.0>风险值≥2.0(比较安全),2.0>风险值≥0.0(非常安全)）
端口数	资产发现或系统扫描任务中扫描出此资产的端口数
风险端口数	资产发现或系统扫描任务中扫描出此资产的风险端口数

弱密码数	口令猜解任务中扫描出此资产的弱密码数
严重漏洞数	系统扫描任务中扫描出此资产的严重漏洞数
高危漏洞数	系统扫描任务中扫描出此资产的高危漏洞数
中危漏洞数	系统扫描任务中扫描出此资产的中危漏洞数
低危漏洞数	系统扫描任务中扫描出此资产的低危漏洞数
信息漏洞数	系统扫描任务中扫描出此资产的信息漏洞数
操作	扫描：对此资产创建系统扫描任务，进入任务配置界面 趋势：查看资产漏洞趋势图 编辑：编辑资产 删除：删除资产

4.1.1 添加网络资产

网络资产有三种方式进行添加：

- **新建网络资产**：点击“新建”按钮，填写资产名称、IP、描述、编号、负责人、主机类型、配置规范等信息进行创建。



新建网络资产参数说明

配置项	描述
名称	网络资产名称
IP	网络资产 IP 地址
描述	资产描述信息
设备编号	资产设备编号

位置	选择资产所在物理位置（省市区）
标签	选择资产标签（标签管理处创建标签）
可信设备	设置资产是否为可信设备
权重	设置资产权重值
选择组织架构	选择资产所属组织架构
所属业务系统	资产所属业务系统名称
网络区域	资产在网络中所属区域（Server、office、DMZ）
负责人	资产负责人姓名
联系方式	资产负责人联系方式
邮箱	资产负责人邮箱号
主机/应用类型	选择资产所属主机/应用类型（做基线检查需要选择主机/应用类型和配置规范）
配置规范	选择资产所属主机/应用类型的配置规范（做基线检查需要选择主机/应用类型和配置规范）
配置规则	提示信息：（大数据组件、中间件配置信息文件路径提示）
目标自动识别	目标自动识别资产所属主机/应用类型的配置规范，需要输入资产 IP 和选择登陆凭证
新建	资产如有多种主机/应用类型，可添加新建配置规范
是否是工控资产	1.选择资产是否为工控资产，如果不是，工控资产扫描的时候则根据通过协议去识别漏洞。 2.选择资产是否为工控资产，如果是，则需要选择设备类型、厂商、型号、版本。系统扫描资产的时候，则根据此处配置的指纹信息进行匹配工控漏洞。
等级保护级别	选择资产等级保护级别
设备机密性:	选择资产保密性级别
设备完整性:	选择资产完整性级别
设备可用性:	选择资产可用性级别
设备重要性：	选择资产重要性级别

- **导入网络资产**：点击“导入”按钮，点击“下载导入模版”，根据模板要求填写资产信息，然后上传模板文件进行资产导入。

★注意：

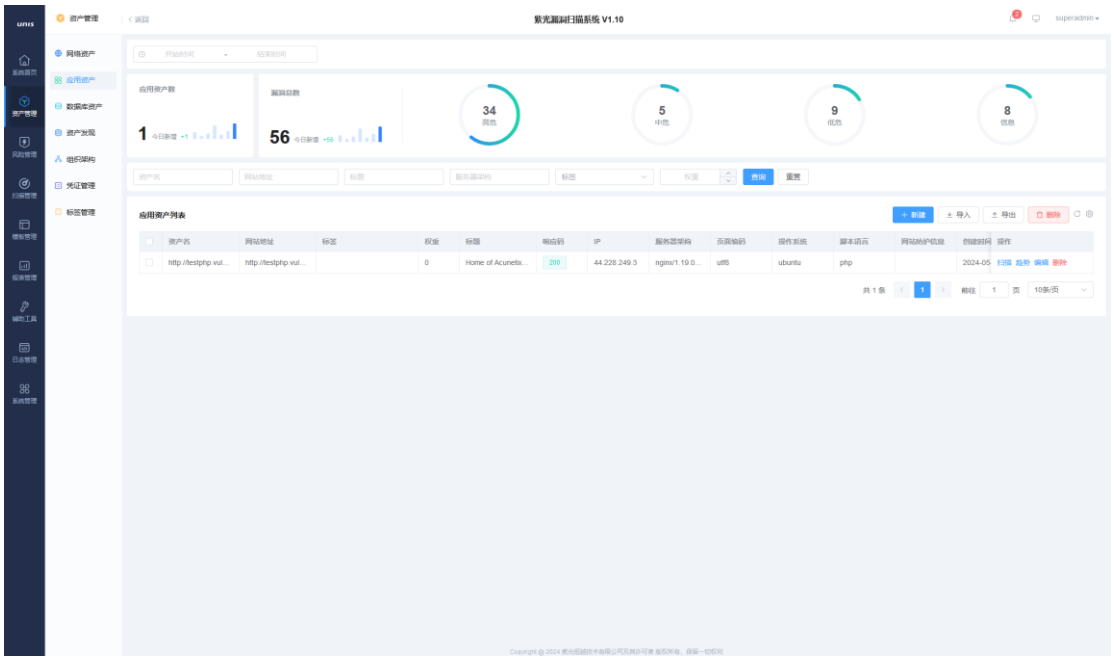
1.对资产进行基线核查时，必须在网络资产中编辑选择资产信息中的主机/应用类型、配置规范，才能正确的进行目标的基线核查。

2. 网络资产进行系统扫描后，将在网络资产列表中，实时展示资产的风险端口、漏洞数量情况。

- **资产发现一键添加**：通过【资产管理】—【资产发现】进行扫描后，可一键将发现的资产信息添加进对应类型的资产中。

4.2 应用资产

应用资产主要用于 web 网站资产的管理，可对 web 资产进行资产信息完善，网络资产录入后，可在应用扫描模块中进行应用资产选择，自动绑定对应资产信息和认证信息进行脆弱性扫描。



资产管理内容参数说明

显示项	描述
资产名	输入要搜索的应用资产名称
网站地址	输入要搜索的应用网站地址
标题	输入要搜索的应用网站标题
服务器架构类型	输入要搜索的应用网站服务器架构类型
标签	选择资产标签进行筛选
权重	展示设置的权重值资产
查询	点击进行搜索
+ 新建	新建应用资产
导入	导入应用资产
导出	导出所有应用资产，格式为 xlsx
删除	删除列表中选中的应用资产

资产列表内容参数说明

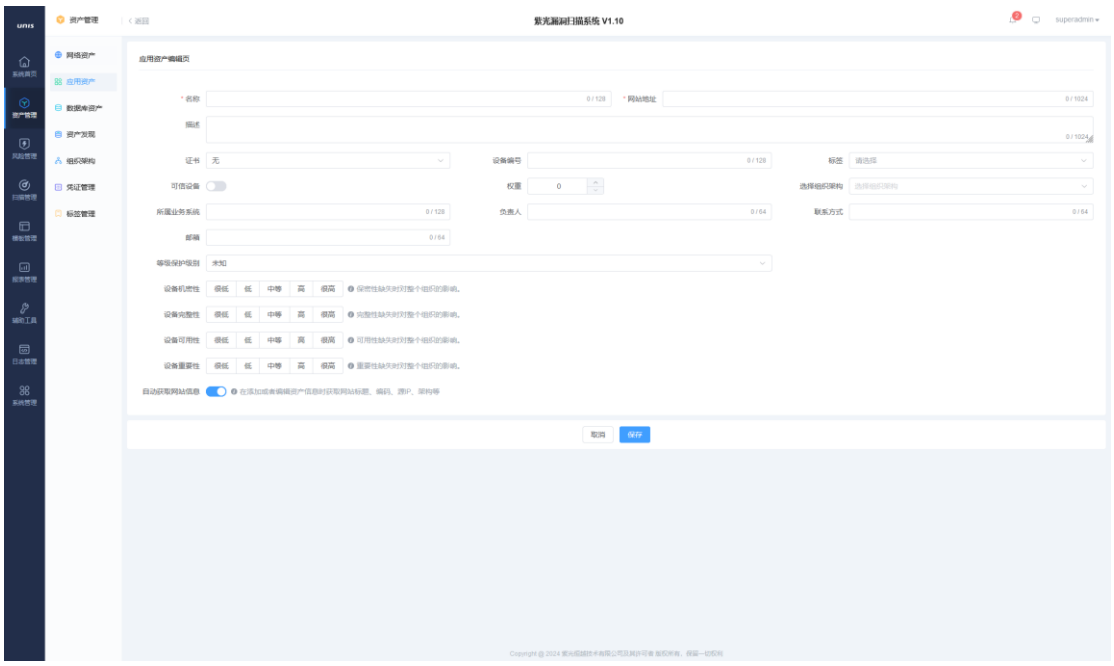
显示项	描述
资产名	应用资产的资产名称
网站地址	应用资产的网站地址信息

标签	资产标签信息
权重	资产权重值
标题	应用的标题信息（应用可访问的情况下，系统会自动获取应用的标题信息）
响应码	web 状态码（系统会自动请求应用获取状态码）
网站 IP	网站的 IP 地址
服务器架构	网站的服务器架构
页面编码	网站的编码方式
操作系统	应用服务器操作系统信息
脚本语言	应用开发脚本语言
网站防护信息	应用网站防护信息
创建时间	应用资产发现/创建时间
操作	扫描：对此资产创建系统扫描任务，进入任务配置界面 趋势：查看资产漏洞趋势图 编辑：编辑资产 删除：删除资产

4.2.1 添加应用资产

应用资产有两种方式进行添加：

- **新建应用资产**：点击“新建”按钮，填写网站名称、网站地址、证书、描述、组织架构、编号、负责人、主机类型、配置规范等信息进行创建。



新建应用资产参数说明

配置项	描述
网站名称	网络资产名称
网站地址	网络资产 IP 地址
描述	资产描述信息
证书	选择认证证书（无、PEM、PFX/P12）
设备编号	资产设备编号
标签	选择资产标签（标签管理处创建标签）
可信设备	设置资产是否为可信设备
权重	设置资产权重值
选择组织架构	选择资产所属组织架构
所属业务系统	资产所属业务系统名称
负责人	资产负责人姓名
联系方式	资产负责人联系方式
邮箱	资产负责人邮箱号
等级保护级别	选择资产等级保护级别
设备机密性:	选择资产保密性级别
设备完整性:	选择资产完整性级别

设备可用性:	选择资产可用性级别
设备重要性:	选择资产重要性级别
获取网站标题:	选择是否打开/关闭自动获取网站标题

- **导入应用资产**：点击“导入”按钮，在导入页面点击“载导入模板”根据模板填写资产信息，然后上传模板文件进行资产导入。

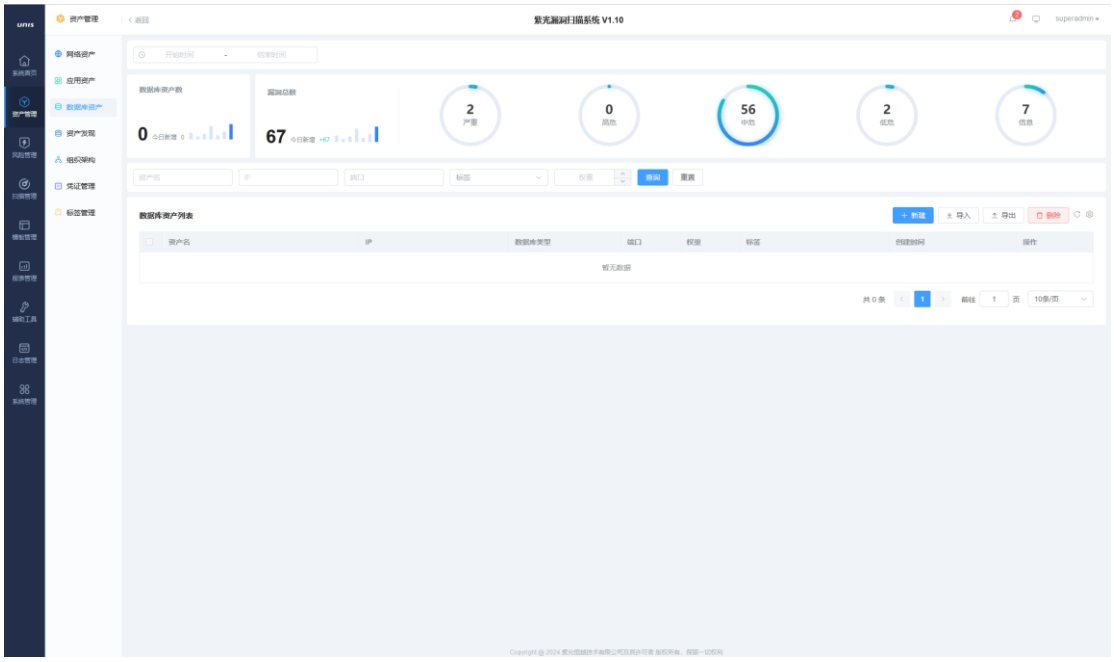
- **资产发现一键添加**：通过【资产管理】—【资产发现】进行扫描后，可一键将发现的资产信息添加进对应类型的资产中。

★注意：

1. 有的网站需要双向认证后才能访问扫描，需要在【模板管理】—【证书管理】创建导入证书信息，然后在应用资产中，编辑资产信息，选择对应的证书。在应用扫描任务中，选择此应用资产，会自动调用证书进行认证扫描。

4. 3 数据库资产

数据库资产主要用于数据库的管理，可对数据库资产进行信息完善，数据库资产录入后，可直接在资产列表发起检查，还可在数据库扫描模块中进行资产选择，自动绑定对应资产信息和认证信息进行脆弱性扫描。



操作区参数说明

显示项	描述
资产名	输入要查找的数据库资产名称
ip	输入要查找的数据库资产 IP
标签	选择资产标签进行筛选
− 权重 +	展示设置的权重值资产
搜索	点击进行搜索
新建	新建数据库资产
导入	导入数据库资产
导出	导出所有数据库资产，格式为 xlsx
删除选中	删除列表中选中的数据库资产

页面显示内容参数说明

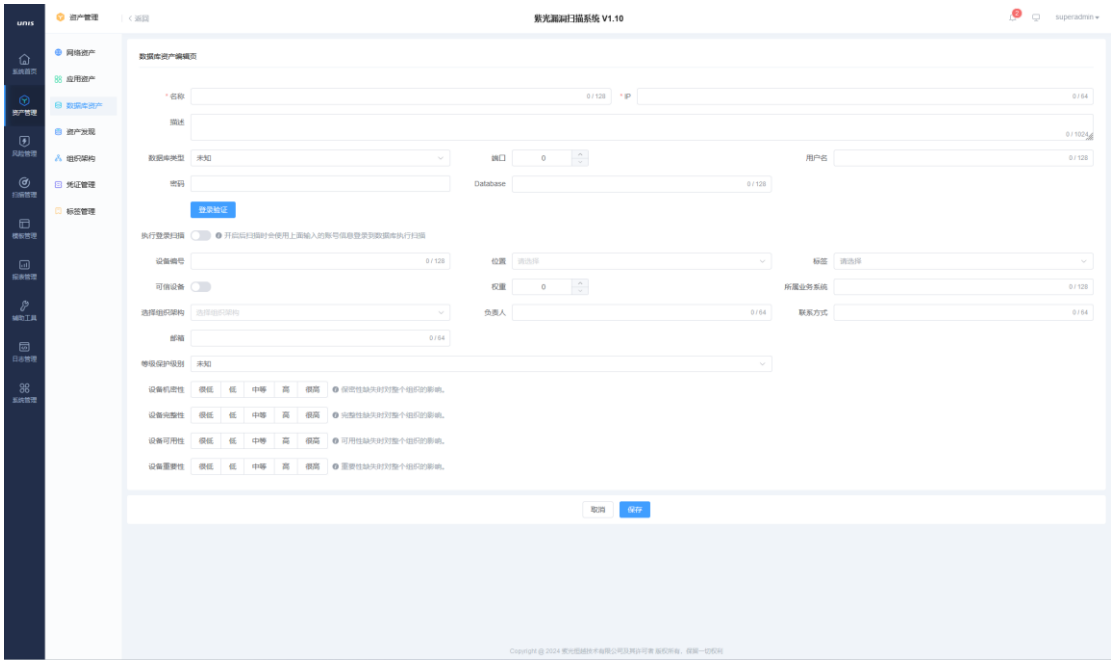
显示项	描述
资产名	此数据库资产的资产名称
IP	此数据库资产的 IP 地址信息
数据库类型	此数据库资产的数据库类型
端口	数据库端口号
权重	资产权重值

标签	资产标签信息
创建时间	数据库资产发现/创建时间
操作	扫描：对此资产创建数据库扫描任务，进入任务配置界面 编辑：编辑资产 删除：删除资产

4.3.1 添加数据库资产

数据库资产有两种方式进行添加：

- **新建数据库资产：**点击“新建”按钮，填写资产名称、数据库地址、数据库类型、端口、用户名、密码、database、执行登录扫描、描述、编号、位置、所属业务系统、组织架构选择、负责人、联系方式、邮箱、等级保护级别、设备保密性、完整性、可用性和重要性级别配置等信息进行创建。



新建数据库资产参数说明

配置项	描述
资产名称	数据库资产名称
IP	数据库资产 IP 地址
数据库类型	数据库类型（下拉框）

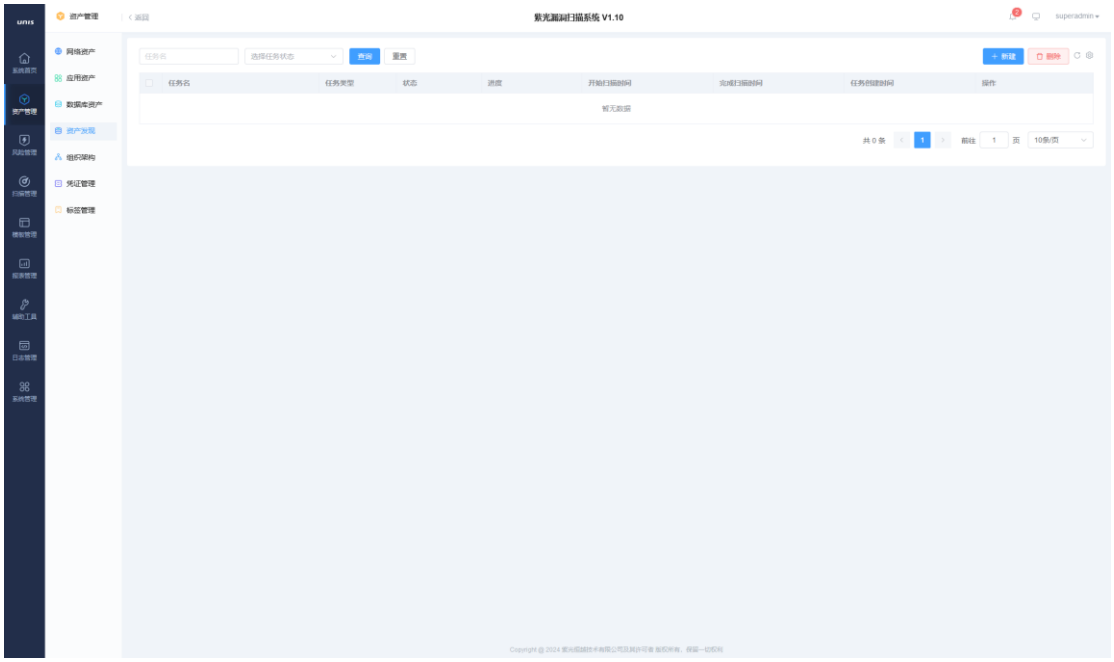
端口	数据库端口号
用户名	登陆数据库用户名
密码	登陆数据库密码
Database	数据库名
登录验证	验证凭证是否正确
执行登录扫描	开启后扫描时会使用上面输入的账号信息登录到数据库执行扫描
描述	数据库资产描述信息
设备编号	资产设备编号
位置	选择资产所在物理位置（省市区）
标签	选择资产标签（标签管理处创建标签）
可信设备	设置资产是否为可信设备
权重	设置资产权重值
选择组织架构	选择资产所属组织架构
所属业务系统	资产所属业务系统名称
负责人	资产负责人姓名
联系方式	资产负责人联系方式
邮箱	资产负责人邮箱号
等级保护级别	选择资产等级保护级别
设备机密性:	选择资产保密性级别
设备完整性:	选择资产完整性级别
设备可用性:	选择资产可用性级别
设备重要性：	选择资产重要性级别

- **导入数据库资产：**点击“导入”按钮，下载导入模板，根据模板要求填写资产信息，然后上传模板文件进行资产导入。

- **资产发现一键添加**：通过【资产管理】—【资产发现】进行扫描后，可一键将发现的资产信息添加进对应类型的资产中。

4.4 资产发现

资产发现支持全网资产自动探测，识别协议、开放端口和服务，同时支持子域名解析；扫描结束后可将资产一键添加到资产库。



4.1.1 创建任务

步骤 1. 创建任务在【资产管理】—【资产发现】中，点击“新建”按钮，进入资产发现任务创建配置页。

资产发现任务参数说明

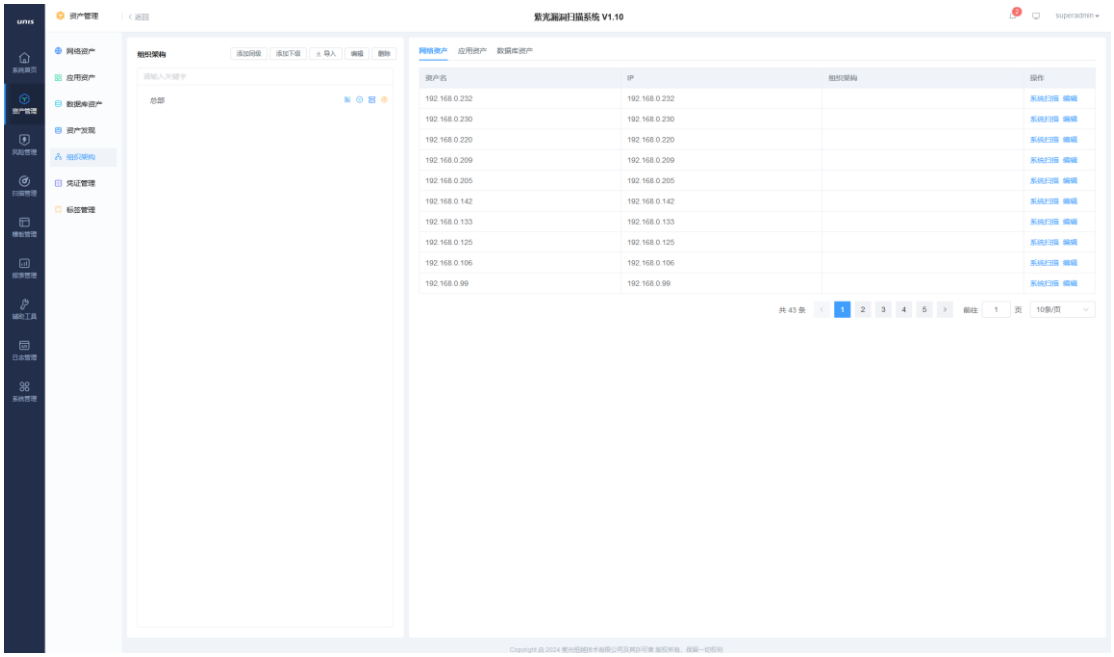
显示项	描述
IP 发现	
*IP	输入需要发现的 IP 信息
端口选择	选择要扫描的端口模板
自定义端口列表	启用后将扫描自定义的端口,不扫描端口模版中的端口
跳过主机发现	勾选后不检查主机是否在线,认为所有主机都是在线的（默认不勾选）
端口扫描模式	**SYN：** 为 TCP SYN(半连接)，扫描器向目标主机的一个端口发送请求连接的 SYN 包，扫描器在收到 SYN/ACK 后，不是发送的 ACK 应答而是发送 RST 包请求断开连接 **Connect：**为 TCP connect(全连接),扫描器会向服务器目标端口发送 TCP 包进行连接完成三次握手,扫描速度比 SYN 慢 **TCP ACK：**扫描主机向目标主机发送 ACK 数据包，根据返回的 RST 数据包有两种方法可以得到端口的信息。 **TCP Null：**反向扫描，通过设置 flags 位为空,不回复则表示端口开启，回复并且回复的标志位为 RS 表示端口关闭，可以辨别某台主机运行的操作系统是什么操作系统 **TCP Xmas：**发送带有标志位的 tcp 数据包，通过设置 flag 位 FPU，如果未回复表示端口开启，如果回复 RA 表示端口关闭 **TCP Window：**检测目标返回的 RST 数据包的 TCP 窗口字段。如果目标端口处于开放状态，这个字段的值将是正值；否则它的值应当是 0。 **TCP Fin：**在 FIN 扫描中一个设置了 FIN 位的数据包被发送后，若响应 RST 数据包，则表示端口关闭，没有响应则表示开放
扫描服务类型	勾选后是识别目标端口所开启的服务例如是 http 还是 mysql,开启后扫描速度会比较慢
扫描工控协议	勾选后会扫描如 mudbus、S7 等工控专业协议
扫描速度	根据并发调整可选择：自适应、快速、超快速
资产发现 IP 结果列表参数说明	
ip	输入需要查找的 IP
端口	输入要查找的端口号

服务	输入要查找的服务名称
搜索	点击进行相应条件筛选
全部添加到资产	将所有结果全部添加到对应的资产里
导出	导出所有结果
IP	发现的资产 IP 信息
端口	资产暴露的端口号
服务	资产暴漏的服务名
组件	资产暴漏的组件名
版本	资产暴漏的组件版本信息
响应码	资产 web 服务的响应码
标题	资产网站标题
首次发现时间	每条记录首次发现的时间
最后发现时间	记录最后一次发现的时间
操作	添加到资产：将资产添加进对应的资产清单 删除：删除这条记录
子域名破解	
*域名	输入需要解析的域名
域名爆破字典	选择域名爆破字典
模版配置	进入域名爆破字典配置页
域名并发数(1-10)：	设置域名解析并发数，默认为‘5’
单域名并发线程数(1-500)：	设置单域名并发线程数，默认为‘100’
域名解析结果列表显示说明	
域名	输入需要筛选的域名信息
搜索	点击根据输入的域名信息对结果进行筛选
全部添加到资产	将所有结果全部添加到对应的资产库里
清空结果	清空当前资产发现结果
域名	域名地址
响应码	web 状态码

标题	应用的标题信息
首次发现时间	首次发现时间
最后发现时间	最后发现时间
操作	添加到资产：将资产添加进对应的资产清单 删除：删除这条记录

4.5 组织架构

组织架构可以进行自定义层级结构，组织架构界面能展示所有已有资产的组织所属情况，同时支持编辑，并且支持对资产发起扫描任务。

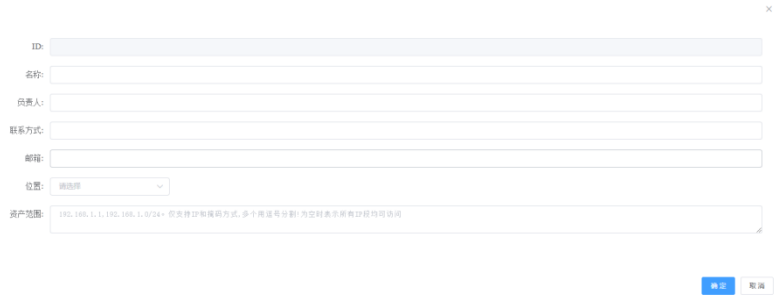


组织架构参数说明

配置项	描述
编辑	选中组织架构的节点后，可以进行编辑
添加同级	选中节点后，添加同级节点
添加下级	选中节点后，添加下级节点
删除	删除选中的节点
导入	下载模板填写后上传导入组织架构，上传时重复的组织结构信息会覆盖老的组织结构信息
网络资产	查看网络资产列表

应用资产	查看应用资产列表
资产名	资产的名称
组织架构	资产所属组织架构
操作	扫描:对资产发起对应的漏洞扫描任务 编辑：编辑资产信息

- 新建部门：选中一个已有的部门，然后根据实际要求选择“添加同级”或者“添加下级”后出现如下页面进行编辑。



组织架构部门编辑页说明

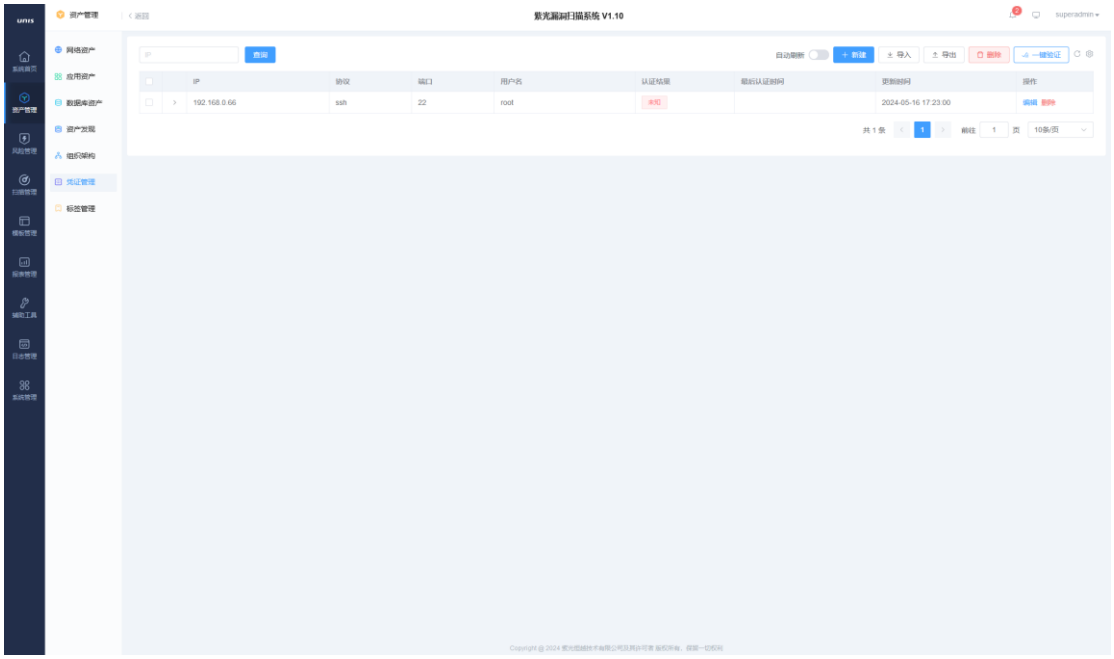
配置项	描述
ID	不可输入，创建后系统会自动生成
名称	节点（部门）名称
负责人	节点（部门）负责人
联系方式	节点（部门）负责人联系方式
邮箱	节点（部门）负责人邮箱号
位置	选择地理位置
资产范围	设置该节点所属资产范围。(192.168.1.1,192.168.1.0/24。仅支持 IP 和掩码方式,多个用逗号分割!为空时表示无所属 IP 范围)

组织架构任务发起说明

操作按钮	描述
	系统扫描：对该部门下所有主机发起系统扫描
	应用扫描：对该部门下所有网站发起应用扫描
	数据库扫描：对该部门下所有数据库发起数据库扫描
	基线核查：对该部门下所有主机发起基线核查任务

4.6 凭证管理

凭证管理用于录入已有资产的登陆访问凭证，用于系统扫描或基线核查时对资产进行登陆扫描。

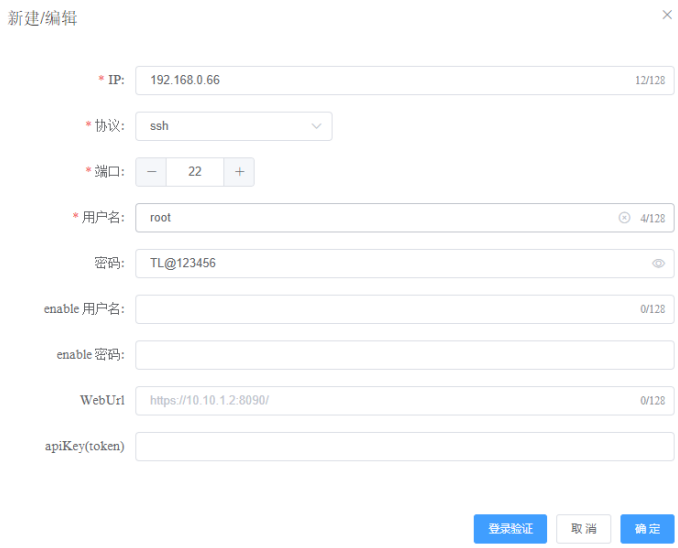


界面参数说明

显示项	描述
IP	输入资产 IP
查询	点击搜索
新建	新建资产凭证
导入	导入资产凭证
导出	导出资产凭证
删除选中	删除选中的凭证
一键验证	一键验证所有凭证（支持 ssh/telnet/smb/winrm/pop3/ftp/snmp）

凭证创建有两种方式：

- **新建凭证**：点击“新建”按钮，录入凭证信息



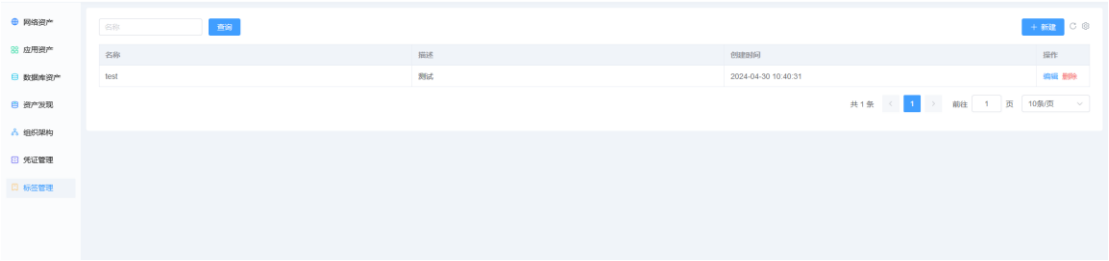
新建凭证参数说明

配置项	描述
IP	资产 IP 地址
协议	远程登陆资产的网络协议（包括：Telnet、ssh、smb、rdp、http、winrm、pop、ftp、snmp 等）
端口	远程登陆资产的端口号
用户名	登陆资产的用户名
密码	登陆资产的用户名密码
enable 用户名	enable 用户名(一般思科设备会有)
enable 密码	enable 用户名密码
WebUrl	资产 Web 访问 URL 地址
apiKey(token)	Api 接口的 token
登录验证	验证凭证/协议是否可正常访问(支持 ssh/telnet/smb/winrm/pop3/ftp/snmp

- **导入凭证：**点击“导入”按钮，然后在弹出的对话框点击“下载导入模版根据导入模块填写凭证信息，然后上传。

4.7 标签管理

标签管理模块用于创建和管理资产标签，标签用于网络资产、应用资产、数据库资产，用户可以对资产进行标签选择，通过标签分类和筛选资产。

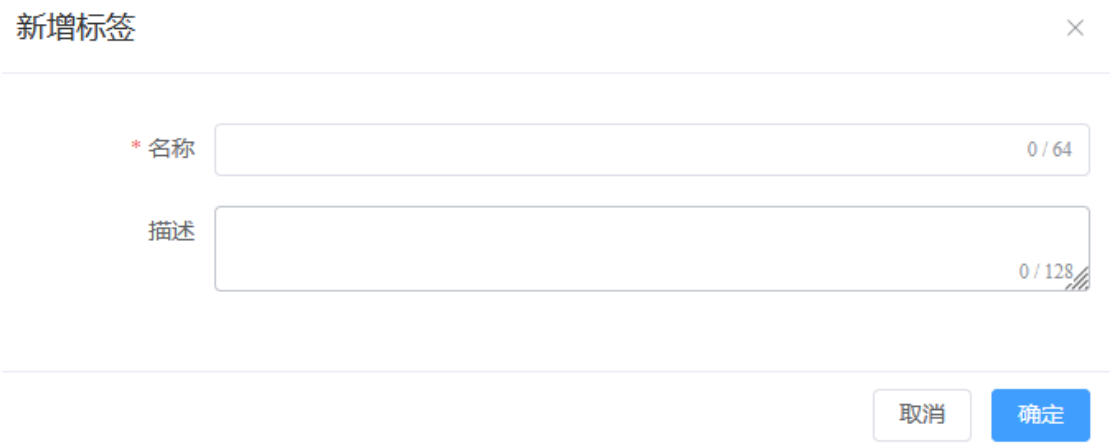


内容参数说明

显示项	描述
名称	输入要查找的标签名称
搜索	点击进行搜索
新建	新建标签
名称	标签名称显示
描述	标签描述内容显示
创建时间	标签创建的时间
操作	编辑：编辑资产 删除：删除资产

4.7.1 添加标签

新建标签：点击“新建”按钮，根据弹出框填写标签名称和标签描述，然后点击“确认”按钮，完成标签创建。

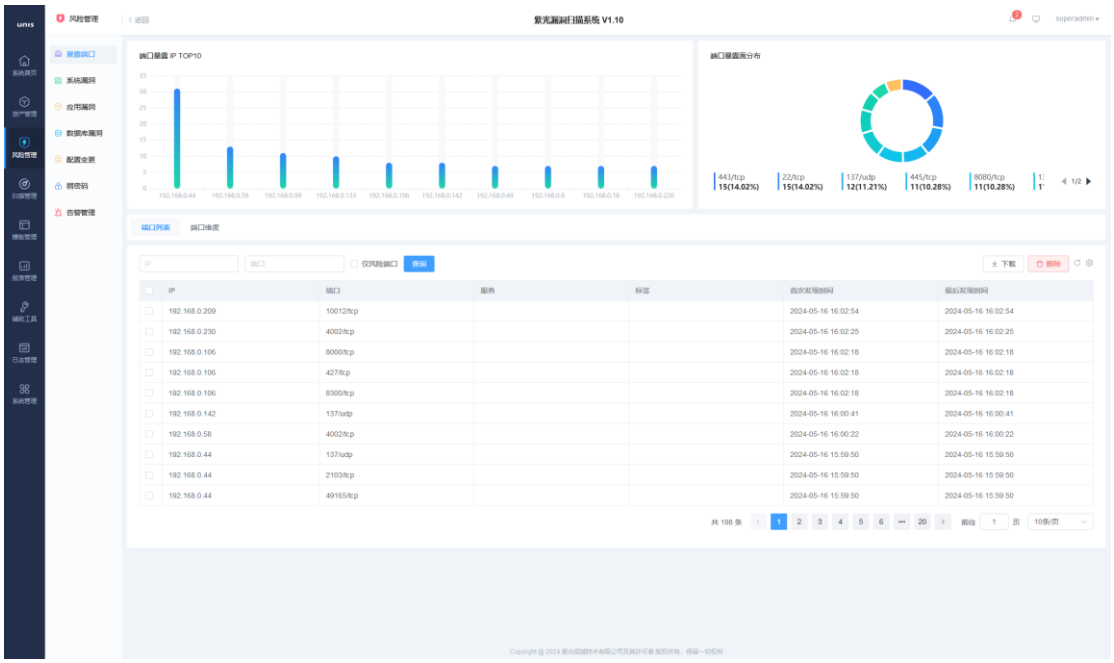


5 风险管理

风险管理包括暴漏端口、系统漏洞、应用漏洞、数据库漏洞、配置变更、弱密码、漏洞情报以及告警管理，用户能够查看所有已扫描的资产的风险情况，包括暴露端口、系统/应用/数据库漏洞情况明细、弱口令风险情况，方便单位或企业记录处理漏洞情况，以及已有漏洞和风险的管理台账功能。

5.1 暴漏端口

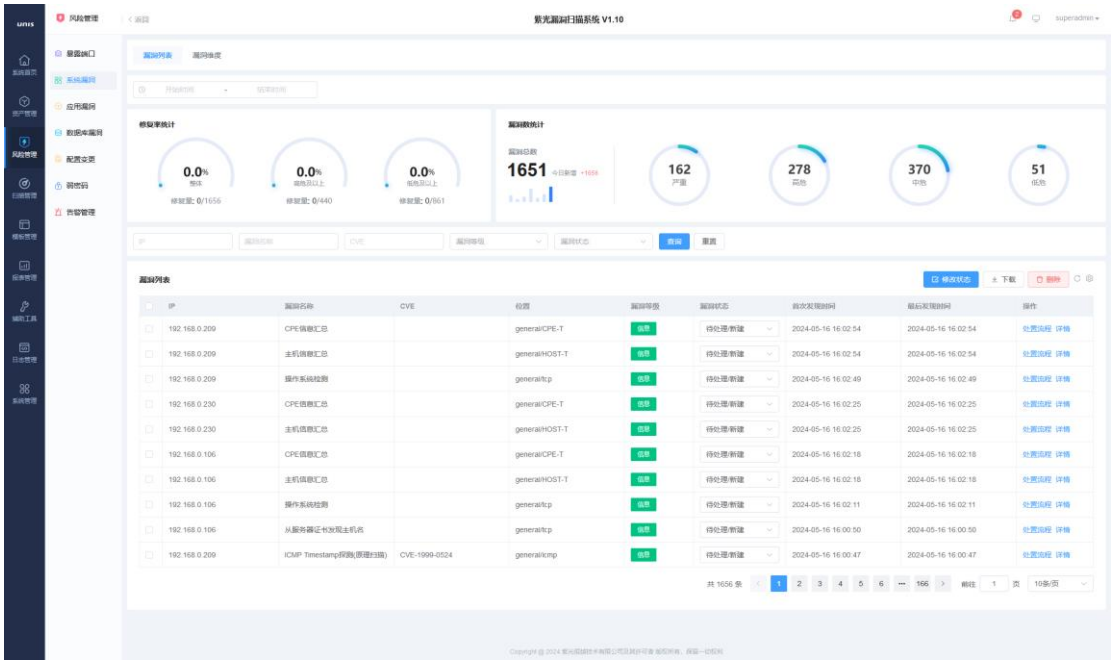
暴漏端口页展示已有资产的所有暴露端口情况，包括 IP 地址、协议、端口号、标签、首次发现时间、最后发现时间等信息，同时不同维度进行查看（端口列表、端口维度）。



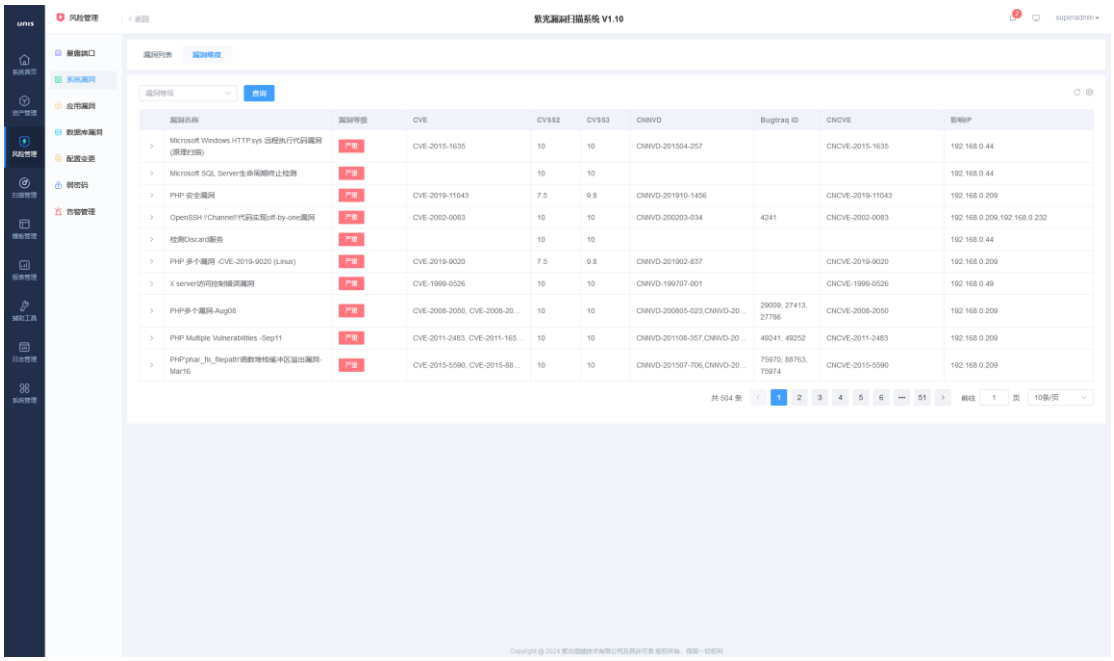
5.2 系统漏洞

通过漏洞列表和漏洞维度展示已有系统资产的所有漏洞情况，包括 IP 地址、漏洞名称、位置、危险等级、漏洞状态、首次发现时间、最后发现时间、漏洞详情（包含漏洞修复建议）以及处置流程等，遵循“漏洞生命周期”原理，记录漏洞从首次发现到修复全流程。

漏洞列表



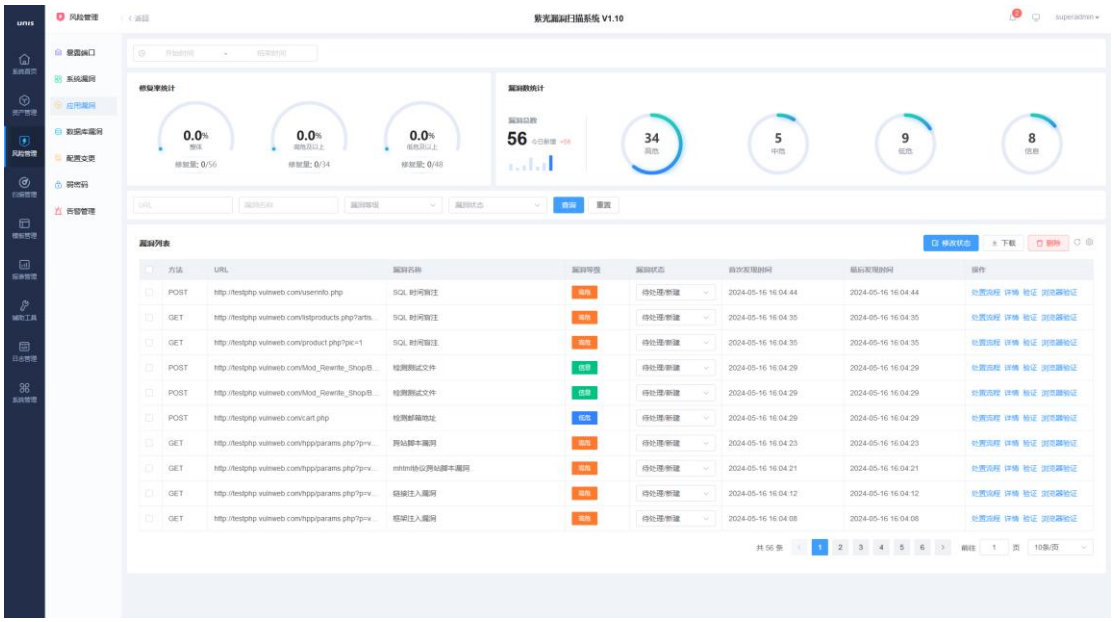
漏洞维度/处置流程



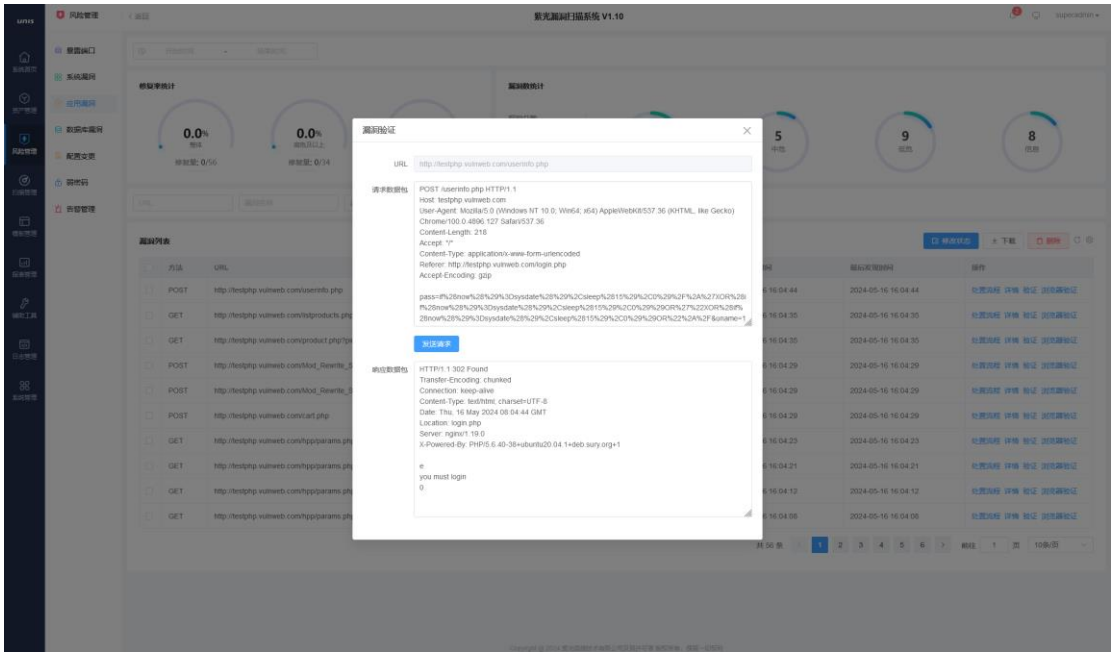
5.3 应用漏洞

通过漏洞列表和漏洞维度展示已有应用资产的所有漏洞情况，包括 URL、漏洞名称、危险等级、漏洞状态、发现时间、漏洞验证、漏洞详情（包含漏洞修复建议）以及处置流程等，遵循“漏洞生命周期”原理，记录漏洞从首次发现到修复全流程。

漏洞列表



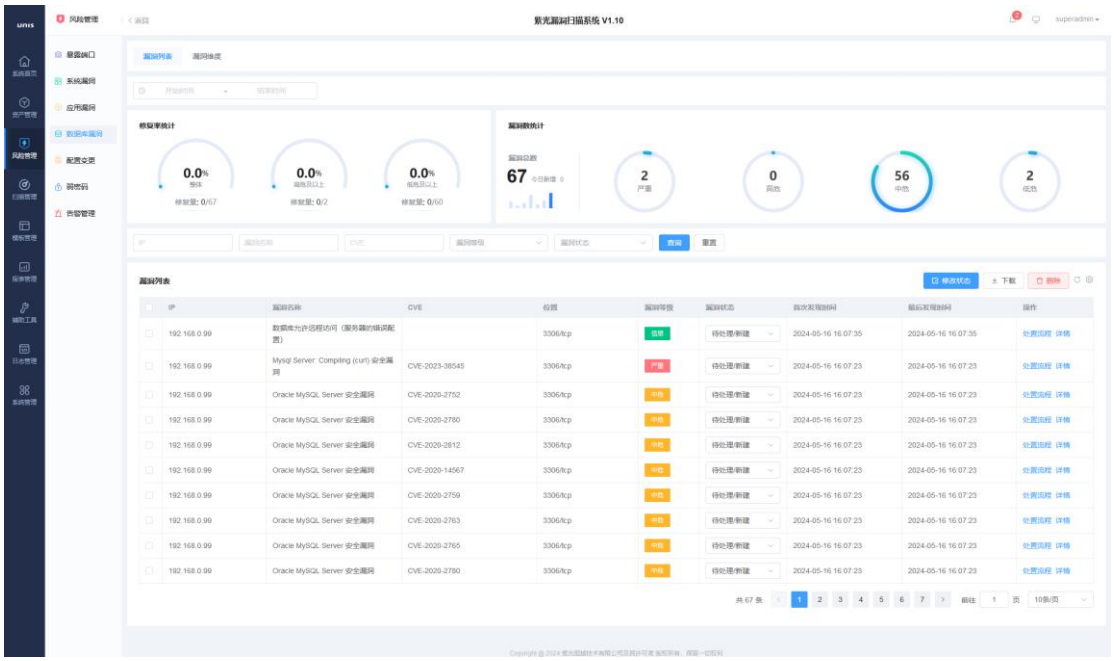
漏洞验证



5.4 数据库漏洞

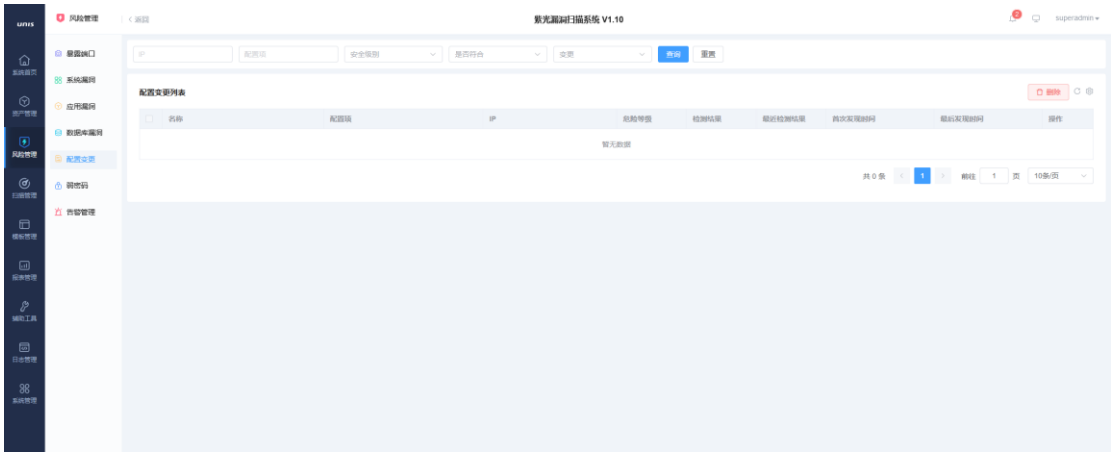
通过漏洞列表和漏洞维度展示已有数据库资产的所有漏洞情况，包括 IP 地址、漏洞名称、位置、危险等级、漏洞状态、首次发现时间、最后发现时间、漏洞详情（包含漏洞修复建议）以及处置流程等，遵循“漏洞生命周期”原理，记录漏洞从首次发现到修复全流程。

漏洞列表



5.5 配置变更

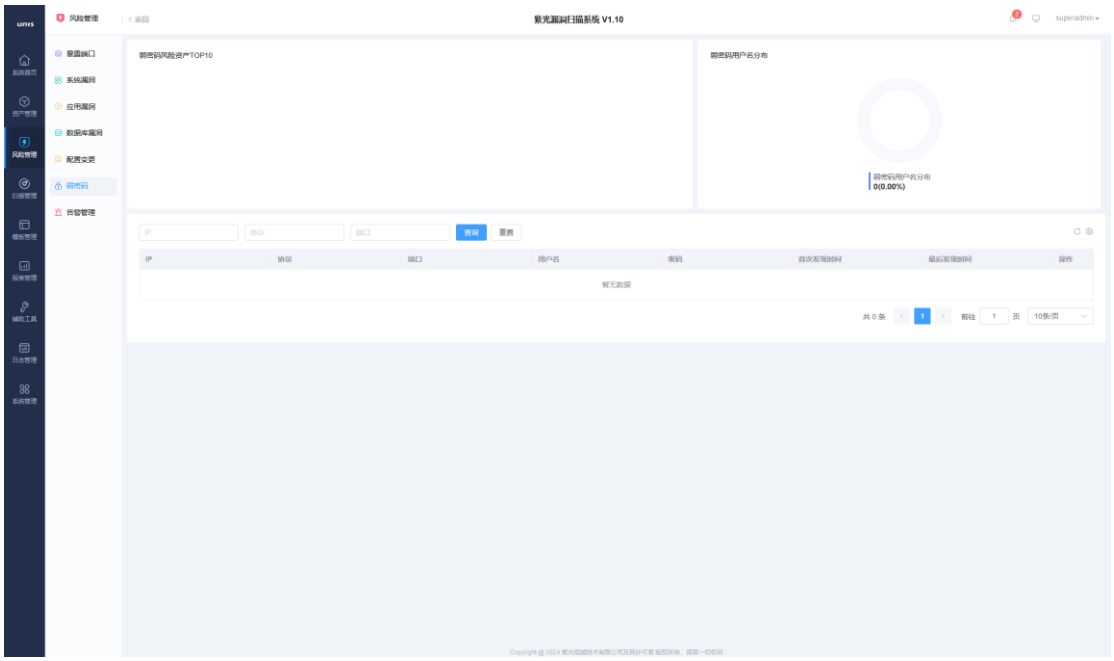
通过配置变更可以快速查看配置核查历史结果，查看初次扫描的配置结果和最后一次的结果对比，可以看到配置结果的变更情况。



5.6 弱密码

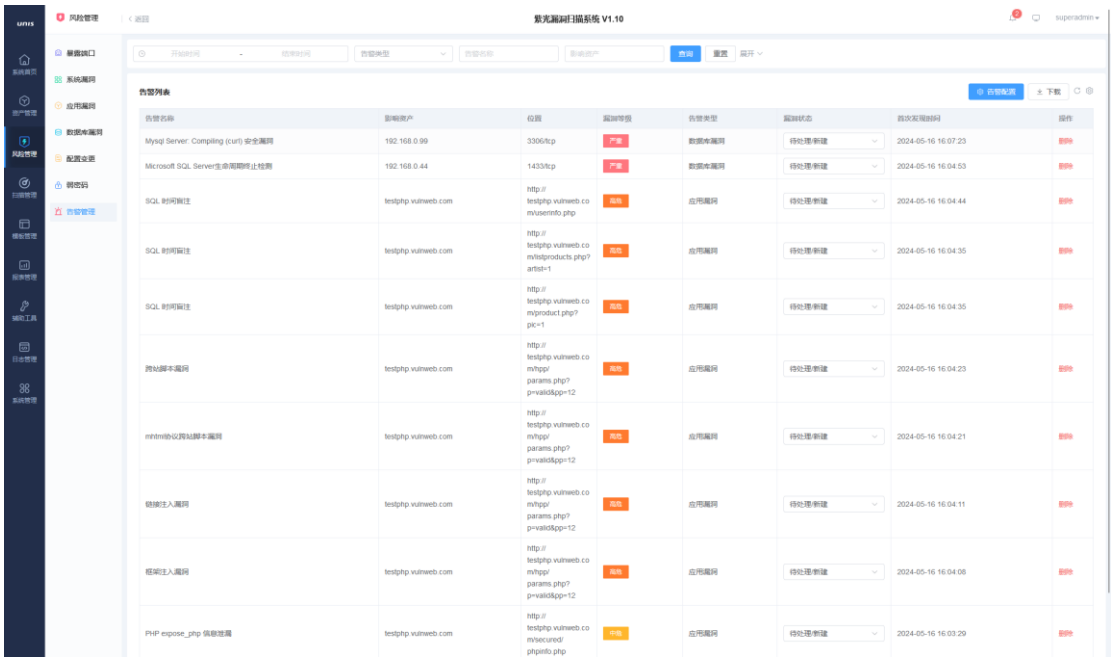
弱口令的一旦被破解将面临很严重的资产风险，在网络安全方面，我们的云主机，服务器一旦暴露了我们的登录密码则会导致我们主机被入侵，导致我们网站，app，主机载体的内容收到损坏，可能导致不可逆的破坏和严重的经济损失。

弱口令风险展示页面通过【风险检测】—【口令猜解】任务结果进行资产弱密码风险展示，可以直观的查看弱密码资产 IP、服务、协议、弱密码等信息。



5.7 告警管理

用户可根据需要配置告警信息可在界面灵活配置告警内容、告警方式告警资产范围等。



界面参数说明

显示项	描述
	选择要筛选的告警类型：系统漏洞、应用漏洞、数据库漏洞、基线配置、弱密码
	输入筛选的告警名称
	输入要查看告警信息的资产 IP/域名
	选择要筛选的漏洞等级
	选择漏洞状态
	点击进行按条件筛选
	进入告警配置页面

6 扫描管理

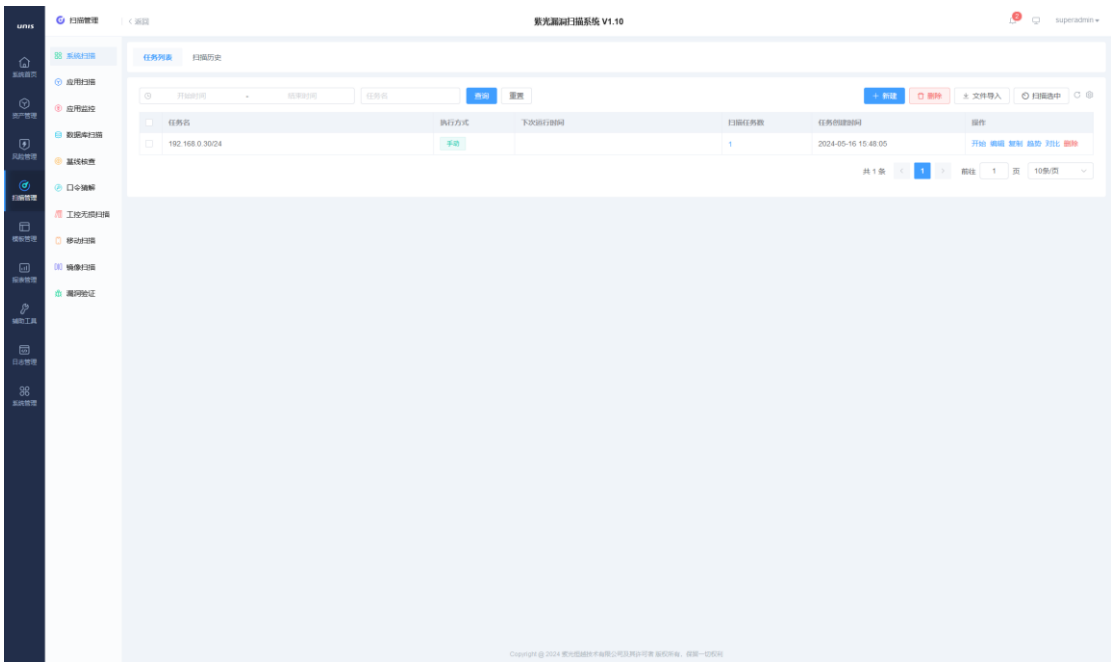
扫描管理为产品的核心功能，涵盖了系统扫描、应用扫描、应用监控、数据库扫描、基线核查、口令猜解、移动扫描、镜像扫描以及漏洞验证模块，全方位的进行各项安全扫描。

本章主要风险检测下十大核心模块的相关信息，主要包括以下内容：

功能	描述
系统扫描	介绍系统扫描任务的管理操作。
应用扫描	介绍应用扫描任务的管理操作。
应用监控	介绍应用监控任务的管理操作
数据库扫描	介绍数据库扫描任务的管理操作
基线核查	介绍基线核查任务的管理操作。
口令猜解	介绍口令猜解任务的管理操作。
移动扫描	介绍移动扫描任务的管理操作。
镜像扫描	介绍镜像扫描任务的管理操作。
漏洞验证	介绍漏洞验证的管理操作。

6.1 系统扫描

系统扫描支持网络中的资产包括：操作系统、数据库、云平台（虚拟化）、工控系统、物联网、大数据组件、网络设备、安全设备等进行漏洞检测。



6.1.1 创建任务

步骤 1. 创建任务在【系统扫描】—【任务列表】中，点击“新建”按钮，进入系统扫描任务创建配置页。

新建系统扫描任务参数说明

配置项	描述	
*任务名称	本次创建系统扫描任务的任务名	
描述	任务描述	
*目标 IP	手动输入 IP：输入目标 IP（支持 IPV6） 手动输入域名：支持对域名解析扫描 IP 主机 网络资产库：从网络资产库中选择要扫描的资产 文件导入：也可通过 txt、、xls、csv 文件进行目标导入	
任务优先级:	根据选择的优先级，后台算法判断执行任务的顺序	
扫描节点:	选择任务扫描节点：auto 表示自动负载均衡,将扫描任务下发到最优的扫描节点。 单机部署时下发到本机。	
执行方式	1. 手动：选择手动开启扫描任务 2. 周期：设置任务扫描周期时间 3. 定时：设置单次扫描定时时间	
参数模版:	选择当前任务的参数模板，可根据不同的任务场景配置模板。	
1. 基础选项		
主机存活探测	跳过主机存活检测	设置是否开启跳过主机存活检测

	主机探测方式	可多选（ARP、ICMP PING、TCP PING、TCP-SYN PING、UDP PING）
	存活探测额外端口	除默认探测端口外，可自定义添加端口号
	存活主机添加到资产库	发现存活主机后，自动添加到网络资产库
端口扫描	端口选择	选择端口模板（可在【模板管理】-【端口管理】中查看和自定义）
	自定义端口列表	启用后将扫描自定义的端口,不扫描端口模版中的端口
	端口扫描方式	选项：TCP ACK、TCP SYN、TCP Connect、TCP Null、TCP Xmas、TCP Window、TCP Fin
	端口扫描速度	1.快速扫描：端口扫描的并发调大，扫描端口速度加快 2.普通扫描：端口扫描的并发正常，扫描端口速度一般
通用设置	漏洞模板选择	选择本次扫描漏洞模板（可在【模板管理】-【系统扫描策略】中查看系统默认模板和自定义新建模板）
	扫描超时后自动停止(分钟):	设置任务扫描时长（分钟），超过此时长，任务自动停止。（为‘0’表示不停止）
2．高级选项		
凭证设置	密码爆破	选择是否开启密码爆破（可在【模板管理】-【字典管理】自定义爆破字典）
	发送扫描通知	选择是否开启发送扫描通知，并可编辑通知内容
	登陆扫描	开启登陆扫描，并选择登陆凭证（登陆凭证可在【资产管理】—【凭证管理】中创建）
	域扫描	支持是否开启域扫描
主机设置	系统扫描顺序	可选择系统扫描顺序（当有多个扫描目标时有效）
	排除扫描主机	设置本次任务不扫描的主机，输入主机 IP 地址
插件设置	漏洞过滤模版选择	选择需要过滤的漏洞模板（默认为空）
	端口扫描超时（秒）	设置扫描端口的超时时长（范围:1-999）
	插件执行超时（秒）	设置漏洞脚本超时时长（范围:1-999）
	网络超时（秒）	设置网络超时时长（范围:1-999）
	运行危险漏洞插件	如果开启则可能执行 Dos 攻击等插件,可能对目标系统产生不良后果
	深度扫描	开启后扫描粒度更细，但是速度也会随之变慢（默认不打开）
并发设置	主机并发数	设置主机并发数（范围为：1-128）

	插件并发数	设置扫描插件并发数（范围为：1-999）
扫描结果	扫描完成后自动生成报表	开启后，选择要生成的报表格式，扫描结束后会在报表管理处自动生成报表
	发送扫描结果到邮箱	扫描结束后，将扫描结果发送至指定邮箱
	发送扫描结果到 FTP	扫描结束后，将扫描结果发送至指定 FTP 服务器
其它设置	扫描工控漏洞	选择是否扫描工控机（1.不扫描 2.仅根据网络资产录入的设备信息做指纹匹配 3.远程扫描）
	扫描打印机	是否开启扫描打印机

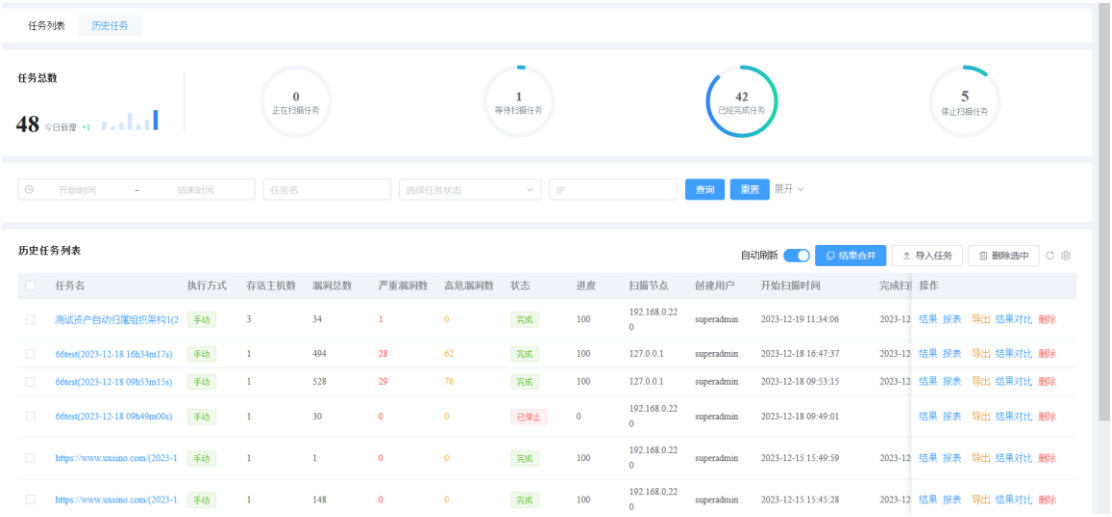
以上配置参数的基础选项和高级选项系统默认为最优配置，使用者可以根据实际情况进行配置修改，配置完成后点击“保存”按钮，即可完成创建,但是任务不会开始扫描；点击“保存并执行”则会完成任务创建并开始进行扫描。

步骤 2.创建任务后，如果执行方式为“手动执行”且没有点击“保存并执行”，需要在任务列表中，在操作栏点击开始扫描按钮，任务则开始进行扫描。

任务列表操作栏说明

操作标题	描述
开始扫描	点击开始此任务扫描。
编辑	编辑此扫描任务的配置参数。
复制	复制此任务，会在任务列表生成一个新任务。
趋势	查看此任务下的所有扫描次数结果进行趋势变化分析。
结果对比	查看此任务下的扫描历史记录进行结果对比。
删除	删除此任务。

步骤 3.在【历史任务】页，可查看当前正在扫描的任务以及历史任务扫描情况，并且支持任务搜索，导入扫描结果，以及批量删除历史任务等功能。



历史任务操作栏说明

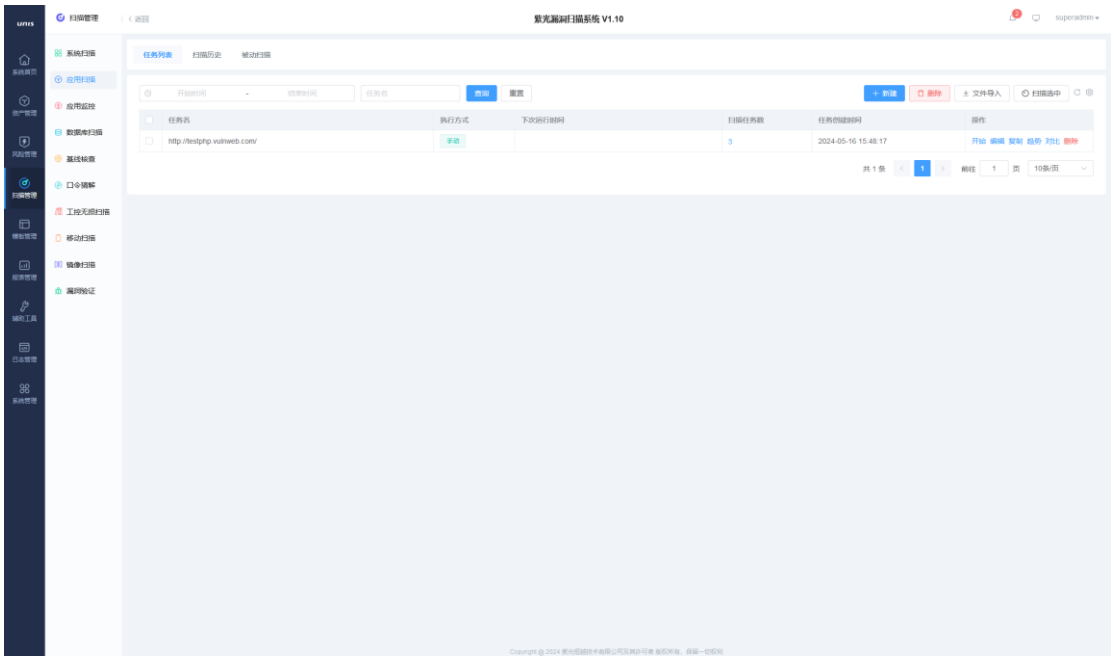
操作按钮	描述
停止	终止此任务。
暂停	暂停此任务
继续	断点续扫，当暂停此任务后，可以进行继续扫描。
结果	此任务的扫描结果预览。
报表	直接跳转到【报表管理】，可以进行此任务的报表生成和下载。
导出	导出此任务扫描结果。
对比	选择任务扫描结果进行横向对比
删除	删除此扫描任务。

★说明：

系统漏洞库数大于 300000 条，用户可以在【模板管理】—【漏洞模板】—【系统扫描】进行查看，同时支持自定义创建漏洞模板。

6.2 应用扫描（主动扫描）

应用扫描支持对主流 Web 漏洞的识别与扫描，包括：SQL 注入漏洞、命令注入漏洞、CRLF 注入漏洞、LDAP 注入漏洞、XSS 跨站脚本漏洞、路径遍历漏洞、信息泄漏漏洞、URL 跳转漏洞、文件包含漏洞、应用程序漏洞、文件上传漏洞等。



6.2.1 创建任务

步骤 1. 创建任务在【应用扫描】—【任务列表】中，点击“新建”按钮，进入应用扫描任务创建参数配置页。

新建应用扫描任务参数说明

配置项	描述
*任务名称	本次创建应用扫描任务的任务名
描述	任务描述说明
*目标 URL	手动输入：输入扫描目标 URL 地址 资产库：从应用资产库选择要扫描的资产
任务优先级:	根据选择的优先级，后台算法判断执行任务的顺序
扫描节点	选择任务扫描节点：auto 表示自动负载均衡，将扫描任务下发到最优的扫描节点。单机部署时下发到本机。
执行方式	1. 手动：选择手动开启扫描任务 2. 周期：设置任务扫描周期时间 3. 定时：设置单次扫描定时时间
会话录制	录制网站的身份信息，可用于登录做深度扫描。
参数模版	选择当前任务的参数模板，可根据不同的任务场景配置模板。
1. 基础选项	

扫描模式	● 先爬行后扫描：先爬取 URL 再扫描 ● 仅爬行：仅爬取 URL 不扫描，可用于查看网站结构 ● 仅扫描：不会爬取 URL，仅扫描当前输入的 URL，通常用于漏洞快速验证	
扫描范围	● 当前域：只扫描目标 URL 下的域名 ● 整个域（含子域名）：扫描目标 URL 下的域名及子域名	
漏洞模板选择	选择此次任务的扫描策略模板	
同一漏洞最大上报个数:	可设置同一种漏洞最大上报个数	
扫描超时自动停止	设置任务扫描时长（分钟），超过此时长，任务自动停止。（为‘0’表示不停止）	
同时扫描域名数	设置任务最大同时扫描的域名数量	
单域名最大并发连接数	并发连接数是指服务器对其业务信息流的处理能力。是服务器能够同时处理的点对点连接的数目，这个参数的大小直接影响到服务器所能支持的最大连接的数目。	
单域名每秒最大请求数	相当于 QPS，每秒最大发送的 HTTP 请求数	
任务优先级	根据选择的优先级，后台算法判断执行任务的顺序	
扫描节点	选择任务扫描节点:auto 表示自动负载均衡,将扫描任务下发到最优的扫描节点	
执行方式	选择手动开启扫描任务、或设置定时开启扫描任务	
扫描超时后自动停止(分钟):	设置任务扫描时长（分钟），超过此时长，任务自动停止。（为‘0’表	
2．高级选项		
HTTP 配置	HTTP 连接超时（秒）	设置连接超时时间
	User-Agent	User-Agent 即用户代理，简称“UA”，它是一个特殊字符串头。网站服务器通过识别 “UA”来确定用户所使用的操作系统版本、CPU 类型、浏览器版本等信息。而网站服务器则通过判断 UA 来给客户端发送不同的页面。例如一个网站通过电脑浏览器打开和通过手机浏览器打开是不同的，大概率就是通过 UA 判断的。
	自定义 Header	HTTP 消息头是指，在超文本传输协议（ Hypertext Transfer Protocol ，HTTP）的请求和响应消息中，协议头部分的那些组件。HTTP 消息头用来准确描述正在获取的资源、服务器或者客户端的行为，定义了 HTTP 事务中的具体操作参数。
登录扫描	认证类型	Basic、Digest 与 NTLM 认证都是基于用户名/密码的认证。

		HTTP Basic:明文传送的用户名与密码信息。 HTTP Digest: 在传输密码前会对其进行 MD5 哈希处理， 同时会配以密码随机数。 NTLM：微软推出的安全协议， 提供了认证、完整性与加密服务。
爬虫配置	爬虫模式	广度优先：把当前页的链接全部爬取完毕再进行下一深度的遍历。 深度优化：爬到一个链接后进一步把它的子链接直到爬去完成，才去爬下一个兄弟链接
	URL 智能去重	如 a/b/c?id=2 a/b/c?id=3 这两个链接，一般页面结构及后台 SQL 都相同，开启后则扫描器只会保留一个链接。
	单域名允许采集的最大链接数	每个域名允许爬取的最大 URL 数。如果网站比较大，例如有上万个链接，那么扫描会特别慢。这种情况可以设置最大链接数，那么采集的链接达到最大链接数后会自动停止采集。
	页面最大爬取深度	A/b/c 表示页面深度为 3，如果该配置为 3，则不会扫描 a/b/c/d 下的链接
	单页面最大接收内容长度(KB)	页面的响应长度，如果设置位 1KB，但是网站的响应长度超过 1KB，就会过滤。
	解析 Flash 文件	是否解析 flash 中的 URL
	执行 JavaScript(浏览器爬虫)	是否执行浏览器爬虫，动态执行 JavaScript
	表单填充内容	配置 HTTP 表单内容
扫描配置	404 页面检测方式	有的网站及时访问的链接不存在，页面也会 200。这种情况需要配置。
	不扫描的链接	一些链接可能是删除、更新、登出的操作，可以通过配置，不扫描这些链接。
	不扫描的后缀	配置不扫描 URL 后缀
	敏感目录字典选择	扫描敏感目录的字典
	死链响应码	判断链接是不是死链，如配置为 500，则网页响应为 500 的话就会判断为是死链。
	连续多次无响应自动停止扫描	连续多次无响应自动停止扫描（默认开启）
	用户名/密码字典	用于表单、后台的密码爆破
代理设置	代理类型	如果扫描器和目标网站网络不通或者要隐藏扫描器的 IP，可以设置代理的方式来扫描

扫描结果	添加存活网站添加到资产库	开启后发现存活网站后，自动添加到应用资产库
	扫描完成后自动生成报表	开启后，选择要生成的报表格式，扫描结束后会在报表管理处自动生成报表
	发送扫描结果到邮箱	扫描结束后，将扫描结果发送至指定邮箱
	发送扫描结果到 FTP	扫描结束后，将扫描结果发送至指定 FTP 服务器

以上配置参数的基础选项和高级选项系统默认为最优配置，使用者可以根据实际情况进行配置修改，配置完成后点击“保存”按钮，即可完成创建,但是任务不会开始扫描；点击“保存并执行”则会完成任务创建并开始进行扫描。

步骤 2. 创建任务后，，如果执行方式为“手动执行”且没有点击“保存并执行”，需要在任务列表中，在操作栏点击“开始”扫描按钮，任务则开始进行扫描。

任务列表操作栏说明

操作标题	描述
开始扫描	点击开始此任务扫描。
编辑	编辑此扫描任务的配置参数。
复制	复制此任务，会在任务列表生成一个新任务。
趋势	查看此任务下的所有扫描次数结果进行趋势变化分析。
删除	删除此任务。

步骤 3. 在【历史任务】页，可查看当前正在扫描的应用扫描任务以及历史任务扫描情况，并且支持任务搜索，导入扫描结果，以及批量删除历史任务等功能。

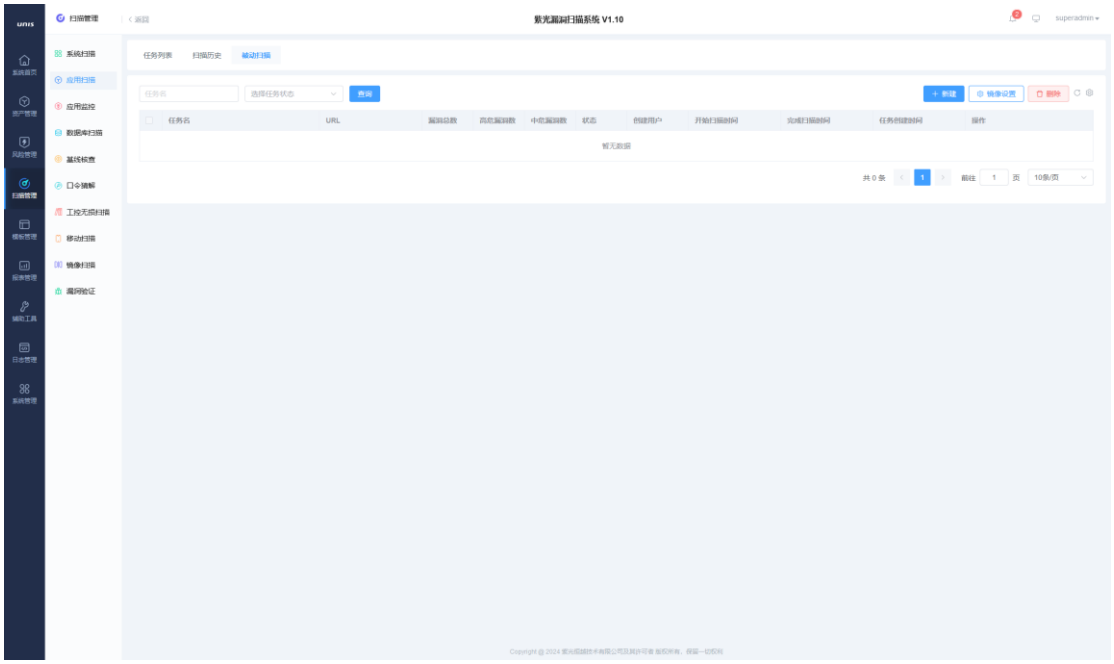
历史任务操作栏说明

操作按钮	描述
停止	终止此任务。
暂停	暂停此任务
继续	断点续扫，当暂停此任务后，可以进行继续扫描。
结果	此任务的扫描结果预览。

报表	直接跳转到【报表管理】，可以进行此任务的报表生成和下载。
导出	导出此任务扫描结果。
对比	选择任务扫描结果进行横向对比
删除	删除此扫描任务。

6.3 应用扫描（被动扫描）

常见的网站漏扫都是主动扫描，也就是先通过爬虫爬到 url 列表再做扫描。这种方式针对传统的 html 页面来说很有效。但是随着前端技术的发展，现在 vue、react 已成为主流，页面基本上都是通过 js 渲染。虽然大多数的扫描器也引入浏览器爬虫去执行 js，但是考虑到页面的复杂性、有的页面需要登录、有的页面需要复杂的逻辑才能触发；所以我们很难通过爬虫的形势去爬到全部的 url，也就无法发现全部的威胁。



被动扫描通过代理、流量等方式实时的抓取流量就可以解决这个问题。例如测试人员在日常功能测试时可以在浏览器配置代理，然后扫描器就可以实时做扫描。

主动扫描和被动扫描对比

扫描方式	主动扫描	被动扫描

操作难度	使用简单，输入 URL 即可扫描	使用较为复杂，但是我们提供了多种接入方式
是否有主动爬虫	是	否，接收到什么扫描什么
需要登录的场景	支持如 basic 等通用认证方式 可以通过 cookie 录制获取登录凭证	只要接收的 http request 中有登陆凭证，就可以实现登录扫描

被动扫描几种方式对比

数据源	特点	使用场景
代理	部署方便，支持 http 和 https	用于日常人工的渗透测试中，如果有自动化测试脚本，只要在测试脚本上配置上扫描的代理即可 对于 QA 人员，日常功能测试时只需要在浏览器配置代理即可
kafka	区分协议，从 kafka 消费到什么扫描什么。 （配置人员需要懂一些开发）	如果有自己的 API 网关或者 WAF 等，可以将流量旁路发送到 kafka 一份，待扫描器消费。
流量镜像	仅支持 http （全流量镜像可能消耗扫描器性能）	N/A
Agent	仅支持 http	部署简单，可以针对性的部署在要扫描的 web 服务器上

6.3.1 创建任务

步骤 1. 创建任务在【应用扫描】—【被动扫描】中，点击“新建”按钮，进入应用扫描任务创建参数配置页。

新建被动扫描任务参数说明

配置项	描述
*任务名称	本次创建应用扫描任务的任务名
描述	任务描述说明
*目标 URL	手动输入：输入扫描目标 URL 地址 资产库：从应用资产库选择要扫描的资产 从文件导入：使用文件导入扫描目标
数据源:	**代理**：支持 HTTP 和 HTTPS，浏览器配置代理后，代理会将 HTTP 请求发送给扫描器做扫描。 **kafka**：支持 HTTP 和 HTTPS，漏扫会从 kafka 消费 HTTP 请求。 **Agent**：仅支持 HTTP，Agent 自动从流量中解析得到 HTTP 请求并发送给扫描器做扫描。 **流量镜像**：仅支持 HTTP，通过交换机将全流量镜像到漏扫的网口后，漏扫会自动从镜像流量中解析得到 HTTP 请求并发送给扫描器做扫描。

1．通用配置	
不扫描链接	一些链接可能是删除、更新、登出的操作，可以通过配置，不扫描这些链接
不扫描后缀	配置不扫描 URL 后缀
根据参数去重	如 a/b/c?id=2 a/b/c?id=3 这两个链接，一般页面结构及后台 SQL 都相同，开启后则扫描器只会保留一个链接
漏洞模板选择	选择此次任务的扫描策略模板
用户名	选择用户名字典
密码	选择密码字典
2．HTTP 配置	
每秒最大请求数（QPS）（1-10000）	相当于 QPS，每秒最大发送的 HTTP 请求数
最大并发连接数（1-1000）	并发连接数是指服务器对其业务信息流的处理能力。是服务器能够同时处理的点对点连接的数目,这个参数的大小直接影响到服务器所能支持的最大连接的数目
HTTP 连接超时（秒）	设置连接超时时间
最大重试次数	设置最大重试次数
User-Agent	User-Agent 即用户代理，简称“UA”，它是一个特殊字符串头。网站服务器通过识别 “UA”来确定用户所使用的操作系统版本、CPU 类型、浏览器版本等信息。而网站服务器则通过判断 UA 来给客户端发送不同的页面。例如一个网站通过电脑浏览器打开和通过手机浏览器打开是不同的,大概率就是通过 UA 判断的。
自定义 Header	HTTP 消息头是指，在超文本传输协议（ Hypertext Transfer Protocol ，HTTP）的请求和响应消息中，协议头部分的那些组件。HTTP 消息头用来准确描述正在获取的资源、服务器或者客户端的行为，定义了 HTTP 事务中的具体操作参数。

kafka（数据源）：配置项

Kafka 集群地址	kafka 的部署地址，个数为 IP:端口，如果是集群的话多个用英文逗号分格
Kafka Topic	流量写入的 topic
消费组名称	唯一值，用来唯一标识消费组
用户名	选填
密码	选填
HTTP Method	json 中值必须为字符串
HTTP Url	json 中值必须为字符串
HTTP Header	json 中值必须为 map[string]string
HTTP Body	必填，json 中值必须为字符串

以上配置参数的基础选项和高级选项系统默认为最优配置，使用者可以根据实际情况进行配置修改，配置完成后点击“保存”按钮，即可完成创建,但是任务不会开始扫描；点击“保存并执行”则会完成任务创建并开始进行扫描。

步骤 2.创建任务后，，如果没有点击“保存并执行”，需要在任务列表中，在操作栏点击开始扫描按钮，任务则开始进行扫描。

任务列表操作栏说明

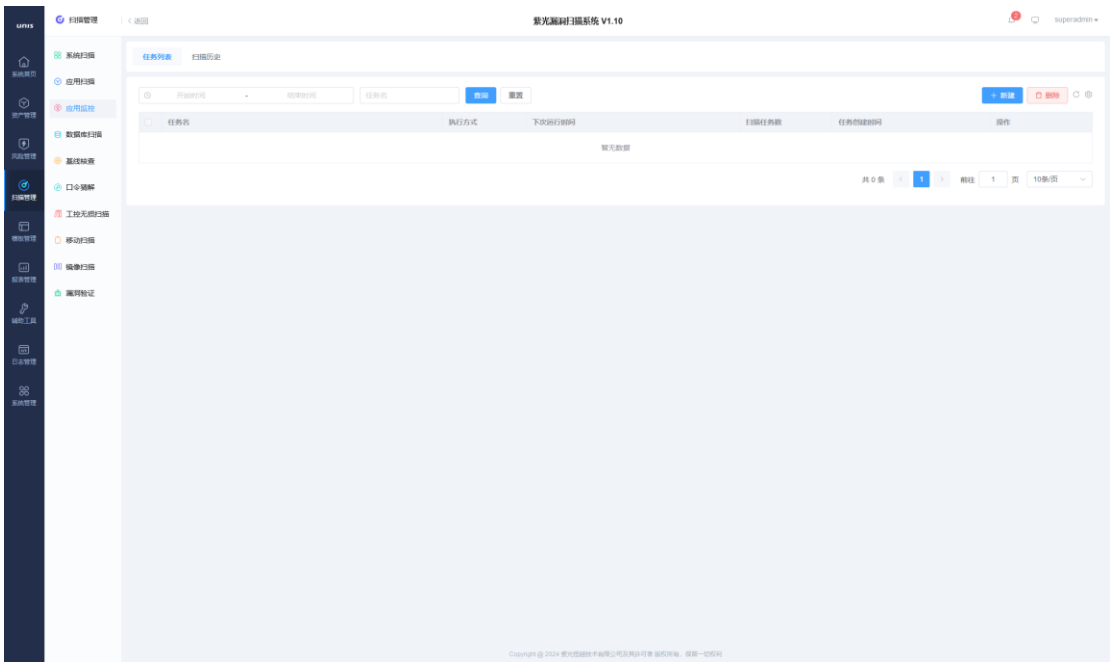
操作标题	描述
开始	点击开始此任务扫描。
停止	终止此任务。
暂停	暂停此任务
继续	断点续扫，当暂停此任务后，可以进行继续扫描。
结果	查看任务扫描的结果信息
报表	点击跳转报表管理，可以生成报表
编辑	编辑此扫描任务的配置参数。
删除	删除此任务。
镜像设置	设置流量镜像的 HTTP 端口号，以及开启关闭流量镜像的接收 注：流量镜像会严重消耗系统性能，不使用时请及时关闭!

★注意:

被动扫描不会有任何的爬虫。接收到多少 URL 就扫描多少 URL。因为扫描器不知道后续会有多少 URL 过来，所以任务就没有所谓的完成状态。

6.4 应用监控

应用监控功能支持对 Web 资产的可用性监控、DNS 解析监控、网页变更监控、关键字监控、暗链挂马监控等功能，方便我们检测 Web 资产的安全运行状态。



6.4.1 创建任务

步骤 1. 创建任务在【应用监控】—【任务列表】中，点击“新建”按钮，进入应用扫描任务创建参数配置页。

新建应用监控任务参数说明

配置项	描述
*任务名称	本次创建应用监控的任务名
描述	任务描述说明
*目标 URL	手动输入：输入扫描目标 URL 地址 资产库：从应用资产库选择要扫描的资产 文件导入：可导入 txt 文件
任务优先级:	根据选择的优先级，后台算法判断执行任务的顺序
扫描节点	选择任务扫描节点：auto 表示自动负载均衡,将扫描任务下发到最优的扫描节点。 单机部署时下发到本机。
可用性监控	
PING 监控	勾选则启用此功能，不勾选则不生效
HTTP 监控	勾选则启用此功能，不勾选则不生效
监控周期	可设置每 N 秒、每 N 分、每小时、多小时、每天、每周、每月等周期自动监控
DNS 解析监控	
启用	勾选则启用此功能，不勾选则不生效

监控周期	可设置每 N 秒、每 N 分、每小时、多小时、每天、每周、每月等周期自动监控
网页变更监控	
启用	勾选则启用此功能，不勾选则不生效
监控周期	可设置每 N 秒、每 N 分、每小时、多小时、每天、每周、每月等周期自动监控
单域名允许采集的最大链接数	每个域名允许爬取的最大 URL 数。如果网站比较大，例如有上万个链接，那么扫描会特别慢。这种情况可以设置最大链接数，那么采集的链接达到最大链接数后会自动停止采集。
页面最大爬取深度	A/b/c 表示页面深度为 3，如果该配置为 3，则不会扫描 a/b/c/d 下的链接
关键字监控	
启用	勾选则启用此功能，不勾选则不生效
监控周期	可设置每 N 秒、每 N 分、每小时、多小时、每天、每周、每月等周期自动监控
关键字字典	选择关键字字典模板，支持自定义
过滤干扰字符	正常看到内容都是 英文和中文， 如果在内容里面插入一些 *& 之类的就会干扰正常的检测，可以设置过滤干扰字符
单域名允许采集的最大链接数	每个域名允许爬取的最大 URL 数。如果网站比较大，例如有上万个链接，那么扫描会特别慢。这种情况可以设置最大链接数，那么采集的链接达到最大链接数后会自动停止采集。
页面最大爬取深度	A/b/c 表示页面深度为 3，如果该配置为 3，则不会扫描 a/b/c/d 下的链接
暗链挂马监控	
启用	勾选则启用此功能，不勾选则不生效
监控周期	可设置每 N 秒、每 N 分、每小时、多小时、每天、每周、每月等周期自动监控
单域名允许采集的最大链接数	每个域名允许爬取的最大 URL 数。如果网站比较大，例如有上万个链接，那么扫描会特别慢。这种情况可以设置最大链接数，那么采集的链接达到最大链接数后会自动停止采集。
页面最大爬取深度	A/b/c 表示页面深度为 3，如果该配置为 3，则不会扫描 a/b/c/d 下的链接
2．高级选项	
User-Agent	User-Agent 即用户代理，简称“UA”，它是一个特殊字符串头。网站服务器通过识别 “UA”来确定用户所使用的操作系统版本、CPU 类型、浏览器版本等信息。而网站服务器则通过判断 UA 来给客户端发送不同的页面。例如一个网站通过电脑浏览器打开和通过手机浏览器打开是不同的，大概率就是通过 UA 判断的。
同时扫描域名数	设置任务最大同时扫描的域名数量
单域名最大并发连接数	并发连接数是指服务器对其业务信息流的处理能力。是服务器能够同时处理的点对点连接的数目，这个参数的大小直接影响到服务器所能支持的最大连接的数目。
单域名每秒最大请求	相当于 QPS，每秒最大发送的 HTTP 请求数

数	
HTTP 连接超时(秒)	设置连接超时时间
不扫描的链接	一些链接可能是删除、更新、登出的操作，可以通过配置，不扫描这些链接
不扫描的后缀	配置不扫描 URL 后缀

配置完成后点击“保存”按钮，即可完成创建,但是任务不会开始扫描；点击“保存并执行”则会完成任务创建并开始进行扫描。

步骤 2.创建任务后，，如果执行方式为“手动执行”且没有点击“保存并执行”，需要在任务列表中，在操作栏点击开始扫描按钮，任务则开始进行扫描。

任务列表操作栏说明

操作标题	描述
开始	点击开始此任务扫描。
编辑	编辑此扫描任务的配置参数。
复制	复制此任务，会在任务列表生成一个新任务。
删除	删除此任务。

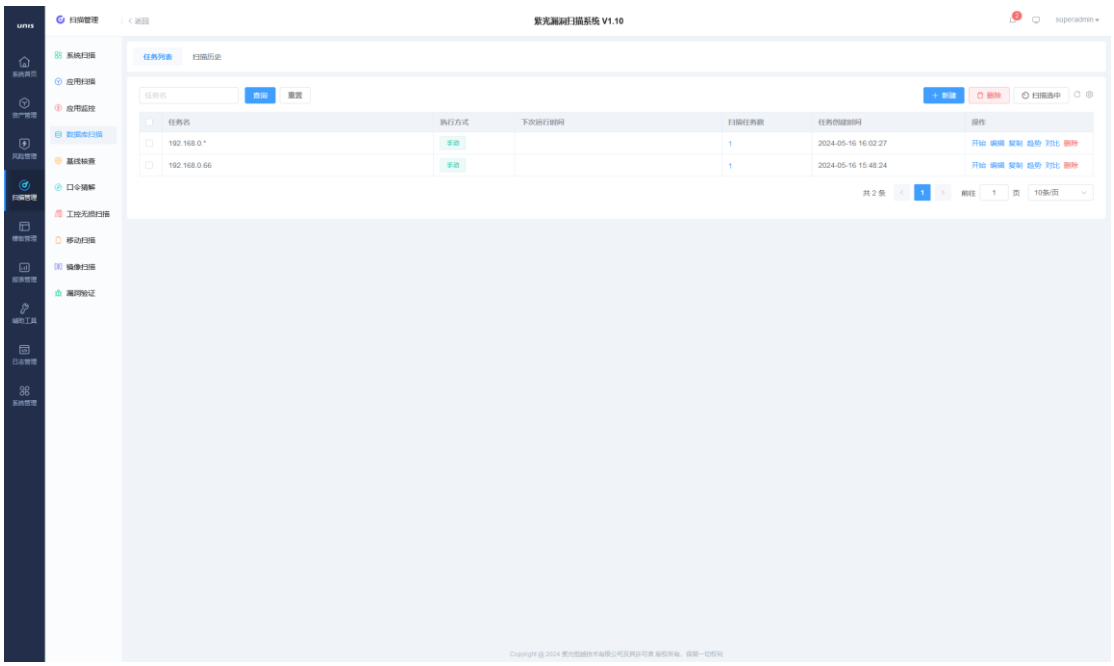
步骤 3.在【历史任务】页，可查看当前正在扫描的应用扫描任务以及历史任务扫描情况，并且支持任务搜索，导入扫描结果，以及批量删除历史任务等功能。

历史任务操作栏说明

操作按钮	描述
停止	终止此任务。
结果	此任务的扫描结果预览。
删除	删除此扫描任务。

6.5 数据库扫描

数据库扫描可对国内外各种关系型和非关系型数据库进行漏洞扫描,同时支持对数据库进行登录扫描，以及数据库的基线配置核查。



6.5.1 创建任务

步骤 1. 创建任务在【应用扫描】—【任务列表】中，点击“新建”按钮，进入应用扫描任务创建参数配置页。

新建数据库扫描任务参数说明

配置项	描述	
*任务名称	本次创建系统扫描任务的任务名	
描述	任务描述	
*目标 IP	手动输入：输入扫描目标数据库地址 资产库（推荐）：从数据库资产库选择要扫描的资产	
任务优先级:	根据选择的优先级，后台算法判断执行任务的顺序	
扫描节点:	选择任务扫描节点:auto 表示自动负载均衡,将扫描任务下发到最优的扫描节点。单机部署时下发到本机。	
执行方式	1.手动：选择手动开启扫描任务 2.周期：设置任务扫描周期时间 3.定时：设置单次扫描定时时间	
参数模版:	选择当前任务的参数模板，可根据不同的任务场景配置模板。	
1．基础选项		
主机存活探测	跳过主机存活检测	设置是否开启跳过主机存活检测
	主机探测方式	可多选（ARP、ICMP PING、TCP PING、TCP-SYN PING）

端口扫描	端口选择	选择端口模板（可在【模板管理】-【端口管理】中查看和自定义）
	端口扫描方式	选项：SYN、Connect
通用设置	漏洞模板选择	选择本次扫描漏洞模板（可在【模板管理】-【系统扫描策略】中查看系统默认模板和自定义新建模板）
	扫描超时后自动停止(分钟):	设置任务扫描时长（分钟），超过此时长，任务自动停止。（为‘0’表示不停止）
2．高级选项		
凭证设置	登录操作系统扫描	如果数据库服务未对外提供，可以通过登录到操作系统的方式查询注册表、软件列表等方式扫描数据
	域扫描	支持是否开启域扫描
主机设置	系统扫描顺序	可选择系统扫描顺序（当有多个扫描目标时有效）
	排除扫描主机	设置本次任务不扫描的主机，输入主机 IP 地址
插件设置	插件执行超时（秒）	设置漏洞脚本超时时长（范围:1-999）,超过这个时间，脚本会自动停止
	网络超时（秒）	设置网络超时时长
	运行危险漏洞插件	如果开启则可能执行 Dos 攻击等插件,可能对目标系统产生不良后果
并发设置	主机并发数	设置主机并发数（范围为：1-128）
	插件并发数	设置扫描插件并发数（范围为：1-999）
扫描结果	扫描完成后自动生成报表	扫描完成后自动将结果生成指定格式报表
	发送扫描结果到邮箱	扫描结束后，将扫描结果发送至指定邮箱
	发送扫描结果到 FTP	扫描结束后，将扫描结果发送至指定 FTP 服务器

以上配置参数的基础选项和高级选项系统默认为最优配置,使用者可以根据实际情况进行配置修改，配置完成后点击“保存”按钮，即可完成创建,但是任务不会开始扫描；点击“保存并执行”则会完成任务创建并开始进行扫描。

步骤 2.创建任务后,，如果执行方式为“手动执行”且没有点击“保存并执行”，需要在任务列表中，在操作栏点击“开始”扫描按钮，任务则开始进行扫描。

任务列表操作栏说明

操作标题	描述
开始扫描	点击开始此任务扫描。
编辑	编辑此扫描任务的配置参数。

复制	复制此任务，会在任务列表生成一个新任务。
趋势	查看此任务下的所有扫描次数结果进行趋势变化分析。
结果对比	查看此任务下的扫描历史记录进行结果对比。
删除	删除此任务。

步骤 3. 在【历史任务】页，可查看当前正在扫描的任务以及历史任务扫描情况，并且支持任务搜索，导入扫描结果，批量删除以及结果合并等功能。

历史任务操作栏说明

操作按钮	描述
停止	终止此任务。
结果	此任务的扫描结果预览。
报表	直接跳转到【报表管理】，可以进行此任务的报表生成和下载。
导出	导出此任务扫描结果。
对比	选择任务扫描结果进行横向对比
删除	删除此扫描任务。

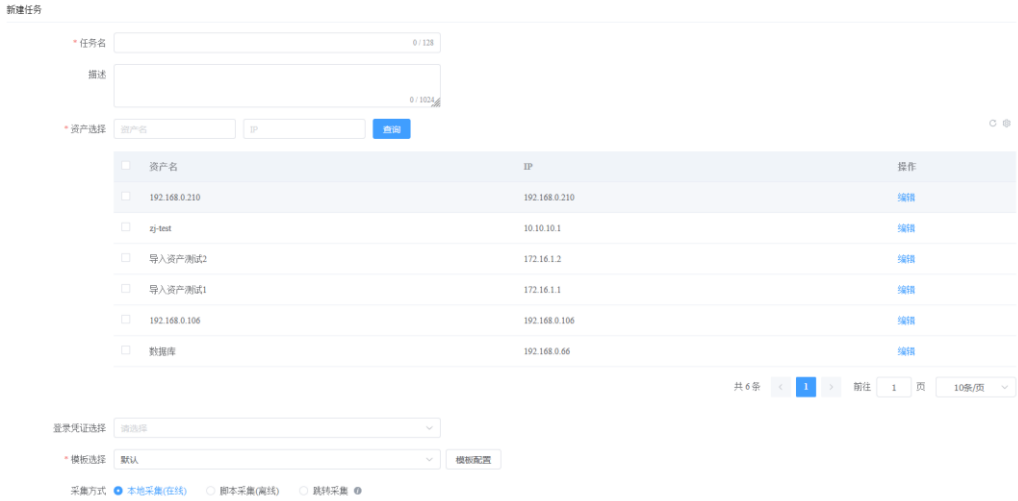
6.6 基线核查

系统支持多种协议远程登录目标系统进行基线核查，包括 SMB、Telnet、SSH 等；采集方式支持本地采集（在线）、脚本采集（离线）、跳转采集三种方式。方便用户及时发现信息系统中存在的不安全配置，提高目标系统的安全防护水平。

6.6.1 创建在线检查任务

在线采集拓扑环境

步骤 1. 创建任务在【基线核查】—【任务列表】中，点击“新建”按钮，进入应用扫描任务创建参数配置页，选择采集方式为“本地采集（在线）”。



★注意：

对目标进行基线核查前，检查目标必须在网络资产中编辑选择资产信息中的主机/应用类型、配置规范，才能正确的进行目标的基线核查。

基线核查任务参数说明

配置项	描述
任务名	本次创建基线核查任务的任务名
描述	任务描述说明
资产选择	选择资产（此处是从网络资产库当中进行选择，可多选）

登陆凭证选择	选择资产登陆凭证（此处是从资产管理-凭证管理当中选择的）
模板选择	选择基线核查的模板（可在模板管理—基线核查策略中进行查看和新建模板）
采集方式	1．本地采集（在线）：通过资产管理模块创建的凭证，进行在线远程自动检测。 2．脚本采集（离线）：创建任务，在基线核查历史任务界面下载插件脚本至目标，执行完把结果传上漏扫平台进行检查。 3．跳转采集支持 Linux 系统：比如漏扫是 A，有个 B 和 C，A 和 B 网络通，B 和 C 网络通，但是要用 A 查 C，这样子就可以通过 B 跳转到 C，前提是 B 上配置了免登录能到 C
任务优先级	根据选择的优先级，后台算法判断执行任务的顺序
执行方式	选择手动开启扫描任务、或设置定时开启扫描任务
扫描超时后自动停止(分钟)：	设置任务扫描时长（分钟），超过此时长，任务自动停止。（为‘0’表示不停止）

步骤 2. 创建任务后，如果执行方式为“手动执行”且没有点击“保存并执行”，需要在任务列表中，在操作栏点击“开始”扫描按钮，任务则开始进行扫描。

任务列表操作栏说明

操作按钮	描述
开始扫描	点击开始此任务扫描。
编辑	编辑此扫描任务的配置参数。
复制	复制此任务，会在任务列表生成一个新任务。
删除	删除此任务。

步骤 3. 在【历史任务】页，可查看当前正在扫描的应用扫描任务以及历史任务扫描情况，并且支持任务搜索，导入扫描结果、结果合并，以及批量删除历史任务等功能。

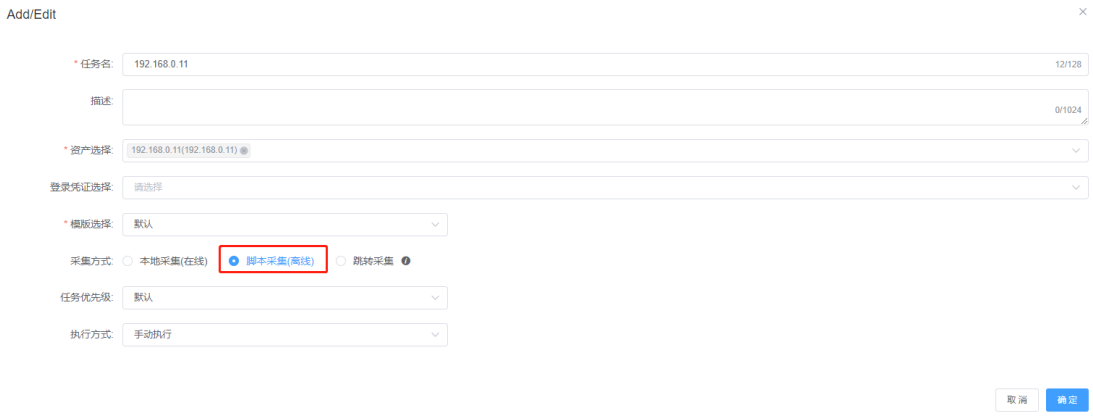
历史任务页操作栏说明

操作按钮	描述
结果	此任务的扫描结果预览。
报表	直接跳转到【报表管理】，可以进行此任务的报表生成和下载。
导出	导出此任务扫描结果。
导入脚本检查结果	离线检查任务情况下，点击此处上传离线检查结果文件
删除	删除此扫描任务。

6.6.2 创建离线检查任务

离线采集拓扑环境

步骤 1. 创建任务在【基线核查】—【任务列表】中，点击“新建”按钮，进入应用扫描任务创建参数配置页，选择采集方式为“脚本采集（离线）”。

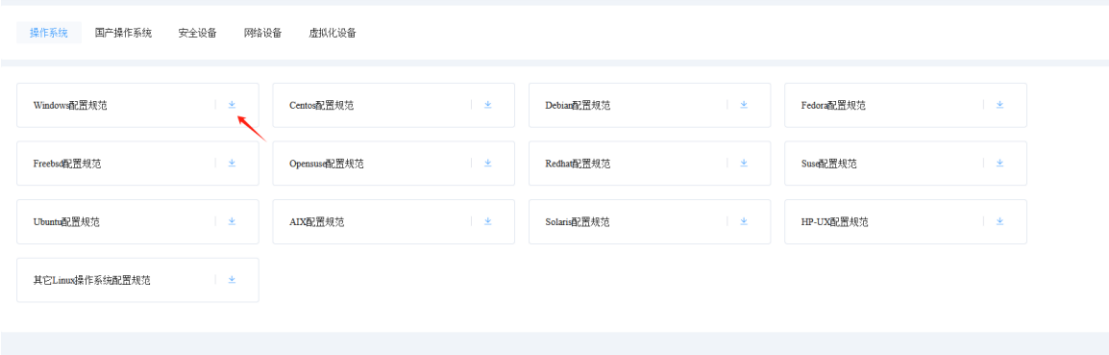


此处可以不用选择登陆凭证，其它参数参考 6.4.1 基线核查任务参数说明，点击确定，即可创建完成。

步骤 2. 创建任务后，如果执行方式为“手动执行”且没有点击“保存并执行”，需要在操作栏点击开始扫描按钮，任务则会启动，在历史任务中会有此任务列表。

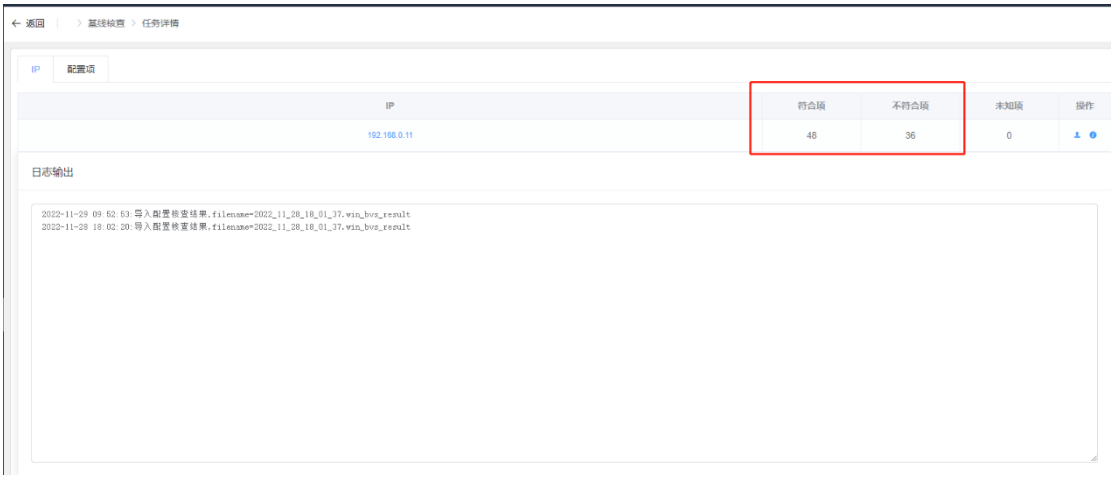
步骤 3. 在【模板管理】—【离线检查工具】中，选择对应检查目标使用的工具或脚本下载到本地，然后到对应的检查目标中运行。

步骤 4. 以检查 windows 操作系统示例，下载离线工具 WindowsBvsAgent.exe 到检查目标中进行安装检查。然后导出结果。

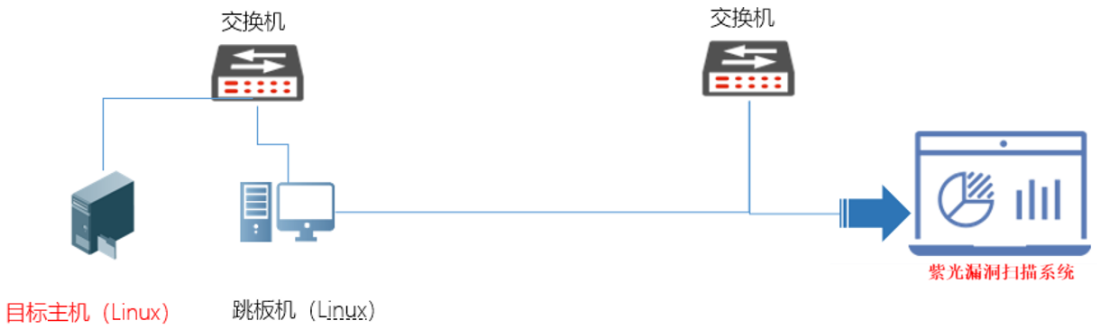


步骤 5. 将导出结果文件上传至【基线核查】-【历史任务】的当前任务里，点击导入脚本检查结果按钮，上传离线检查结果，进行基线检查 。

任务检查成功结果



6.6.3 创建跳转检查任务



跳转采集拓扑环境

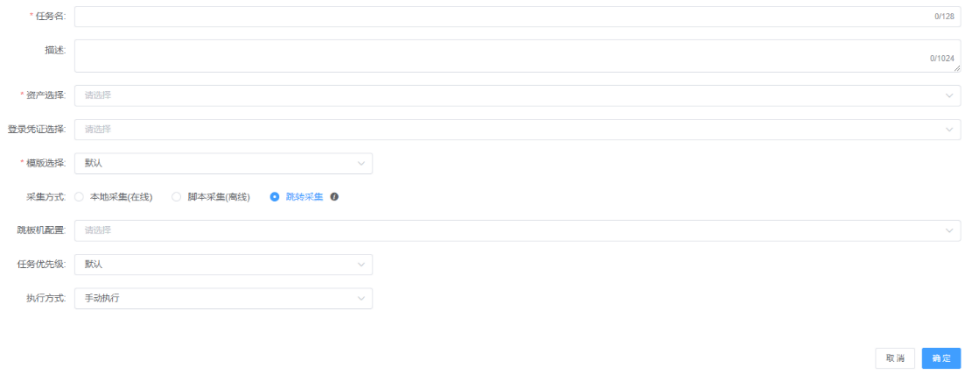
当扫描器无法直接访问被检查目标，可以通过跳板机的方式进行跳转采集，如：扫描器是 A，检查目标是 C，有个 B 和 C，A 和 B 网络通，B 和 C 网络通，但是要用 A 查 C，这样子就可以通过 B 跳转到 C，前提是 B 上配置了免登录能到 C。

步骤 1. 创建任务在【基线核查】—【任务列表】中，点击“新建”按钮，进入应用扫描任务创建参数配置页，选择采集方式为“跳转采集”。

★注意：

1、跳转采集只支持 Linux 操作系统和部分国产化操作系统；

2、**“登陆凭证”不需要选择。**



“资产选择”为检查目标资产，“跳板机配置”选择跳板机的凭证

步骤 2. 在跳板机上配置：

a. ssh-keygen -t rsa 然后回车

b. 生成 sshkey，生成后会在./ssh 目录下 生成 id_rsa 和 id_rsa.pub 密钥文件。

步骤 3. 在被检查目标主机上配置：

a. 创建/.ssh 目录和 authorized_keys 文件并赋权，命令如下：

```
mkdir /.ssh
touch /.ssh/authorized_keys
chmod -R 600 /.ssh
```

步骤 4. 将跳板机上 id_rsa.pub 文件内容复制到被检查主机的 authorized_keys 文件中

步骤 5. 以上配置完成后，到【基线核查】—【任务列表】中，选择当前跳转采集的任务，如果执行方式为“手动执行”且没有点击“保存并执行”，需要点击 按钮开始检查任务，然后到【历史任务】中查看此任务检查进度，待检查进度到 100 时，查看检查结果。

6.7 口令猜解

口令猜解模块提供在线弱口令猜解功能和离线 Hash 爆破，用户可以使用系统内置字典以及自建字典对数据库、服务、中间件等各类猜解对象进行弱口令的猜解，及时发现系统中存在的弱口令，保证系统及服务安全。

口令猜解模式

模式名称	描述
标准模式	用户选择用户名/密码字典进行猜解。
组合模式	用户创建组合字典后，选择组合字典进行猜解

在线破解支持的服务协议

类型名称	描述
常见服务	SMB、Telnet、SSH、IMAP、SNMP、FTP、POP3、SMTP、WinRm、RDP、REXEC、RLOGIN、RTSP、VNC 等
数据库	ClickHouse 、Dameng(达梦):、DB2、ElasticSearch、HighGo(瀚高)、kingbase(金仓)、MongoDB、MSSQL、MySQL、Oracle、PostgreSQL、Redis、STDB(通)、Sybase、UXDB(优炫)等
中间件	ActiveMQ Console、JBoss、Tomcat、WebLogic 等
视频监控	大华、海康、Onvif、SIP 等
HTTP	HTTP Basic

离线 Hash 破解支持的类型

类型名称	使用方法
linux	将/etc/passwd 和 /etc/shadow 下载到本地后，压缩为.zip 上传即可。主要 passwd 和 shadow 需要在根目录且文件名不要改变。
Mysql(SHA1)	登录 mysql 执行:SELECT authentication_string from mysql.user(5.7 以前的版本执行 SELECT password from mysql.user),将返回值放到 txt 上传即可。
Mysql(SHA256)	

MD5、SHA1、SHA256、SHA512	将 hash 值放在 txt 文件上传即可，多个用换行分割，建议一个文件放一个。

★说明：

Hash 函数常用于密码的保存，离线 Hash 爆破即使用字典中的密码经过 Hash 后与目标 Hash 对比，如果相同则成功。所以前提需要拿到密码保存的 hash 值。

6.7.1 创建在线爆破任务

步骤 1. 创建口令猜解任务前，需要在【模板管理】—【字典管理】中，创建用户名字典和密码字典，用于口令猜解。

步骤 2. 创建口令猜解任务，在【口令猜解】—【任务列表】中，点击“新建”按钮，进入口令猜解任务创建配置页。

口令猜解任务配置参数说明

配置项	描述
*任务名称	本次创建口令猜解任务的任务名
描述	任务描述
*目标 IP	口令猜解目标 IP 地址
任务优先级	根据选择的优先级，后台算法判断执行任务的顺序
模式	标准模式：选择用户名/密码字典进行猜解 组合模式：用户创建组合字典后，选择组合字典进行猜解

用户名字典选择	全局选择猜解用户名字典（可在【模板管理】—【字典管理】中自定义） （如果对应的服务选择了用户名密码字典则优先使用服务选择的）
密码字典选择	全局选择猜解的密码字典（可在【模板管理】—【字典管理】中自定义） （如果对应的服务选择了用户名密码字典则优先使用服务选择的）
并发 IP 数	任务同时扫描猜解的 IP 并发数设置
单 IP 并发线程数	单个 IP 同时扫描的线程数
时间间隔	两个扫描线程的时间间隔，默认 0 表示执行完一个立即执行下一个
扫描全部弱密码	默认关闭表示发现一个弱密码即停止扫描,开启后会扫描整个字典中所有的账号密码。
服务协议选择	1.可选择猜解常见服务协议包括：FTP、IMAP、POP3、RDP、REXEC、RLOGIN、RTSP、SMTP、SMB、SNMP、SSH、Telnet、VNC、WinRm 等。 2.可选择猜解数据库包括 ClickHouse 、Dameng(达梦):、DB2、ElasticSearch、HighGo(翰高)、kingbase(金仓)、MongoDB、MSSQL、MySQL、Oracle、PostgreSQL、Redis、STDB(神通)、Sybase、UXDB(优炫)等。 3. 可选择猜解中间件包括:ActiveMQ Console、JBoss、Tomcat、WebLogic 等。 4.支持 HTTP Basic、Grafana、phpMyAdmin、HTTP Form 弱口令猜解 5.支持视频监控设备如大华、海康、华为、联想、Onvif 协议、SIP 协议等。

步骤 3.创建任务后，没有点击“保存并执行”时，需要在操作栏点击 开始扫描按钮，任务则开始进行扫描。

任务列表操作栏说明

操作按钮	描述
开始扫描	点击开始此任务扫描。
编辑	编辑此扫描任务的配置参数。
复制	复制此任务，会在任务列表生成一个新任务。
趋势	查看此任务下的所有扫描次数结果进行趋势变化分析。
删除	删除此任务。

步骤 4.在【历史任务】页，可查看当前正在扫描的应用扫描任务以及历史任务扫描情况，并且支持任务搜索以及批量删除历史任务等功能。

历史任务页操作栏说明

操作按钮	描述
停止	终止此任务。
结果	此任务的扫描结果预览。
下载 xlsx 报表	下载 xlsx 格式结果报表（密码以*代替）
删除	删除此扫描任务。

步骤 5. 口令猜解任务状态显示完成后，点击操作栏上的结果查看按钮，即可查看此任务结果详情。

6.7.2 创建离线 Hash 爆破任务

离线 Hash 爆破任务配置参数说明

配置项	描述
*任务名称	本次创建口令猜解任务的任务名
描述	任务描述
*猜解模式	选择离线 Hash 爆破
任务优先级	根据选择的优先级，后台算法判断执行任务的顺序
密码字典选择	全局选择猜解的密码字典（可在【模板管理】—【字典管理】中自定义）

新建目标参数说明	
IP	输入目标 IP 地址
类型	选择 Hash 类型
输入	选择输入，需要手工输入 Hash 值
上传	选择上传，需要将 Hash 值文件上传至任务中

6.8 移动扫描

系统支持对 Android、IOS 系统上的移动应用（APP）进行漏洞扫描，采用静态分析的方式，准确发现 APK 中存在的组件安全、配置安全、数据安全和恶意行为等安全风险。

6.8.1 创建移动扫描任务

步骤 1. 创建任务在【移动扫描】—【任务列表】中，点击“新建”按钮，进入移动扫描任务创建参数配置页，如下图：

根据 APP 应用包系统类型，选择 Android 或 IOS，然后上传移动应用包，完成后，点击“上传并扫描”后，开始扫描，任务栏此任务扫描状态为：检测中。

步骤 2. 当任务栏中任务状态更新为“完成”后，表示扫描任务已完成，可以在任务操作栏中进行扫描结果的查看和其它操作。

移动扫描任务操作栏说明

操作按钮	描述
APP	将此任务检查 APP 下载到本地
扫描结果	此任务的扫描结果查看
Html 报表	下载此任务扫描结果 html 报表
Doc 报表	下载此任务扫描结果 doc 报表
删除	删除此扫描任务

步骤 3. 移动扫描任务状态显示完成后，点击操作栏上的扫描结果，即可查看此任务结果详情。

6.9 镜像扫描

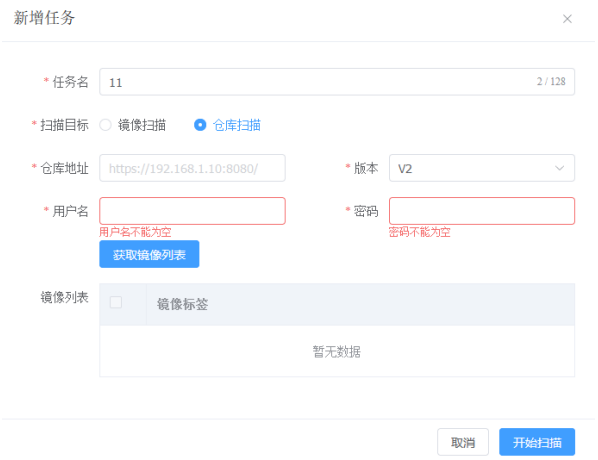
系统支持直接输入镜像标签扫描、支持 dockerhub 私有仓库扫描、支持输入 harbor 仓库信息自动拉取镜像列表并扫描，支持获取镜像中包列表，包括包名、版本、license 信息，支持获取镜像漏洞列表，包括漏洞名称、CVE、等级、描述、建议等。

6.9.1 创建镜像扫描任务

镜像扫描任务分为镜像扫描和仓库扫描，用户根据实际环境选择不同的扫描方式。

步骤 1. 创建任务在【镜像扫描】—【任务列表】中，点击新建按钮，进入镜像扫描任务创建参数配置页。

扫描目标为镜像扫描如下图：



扫描目标为“镜像扫描”参数说明

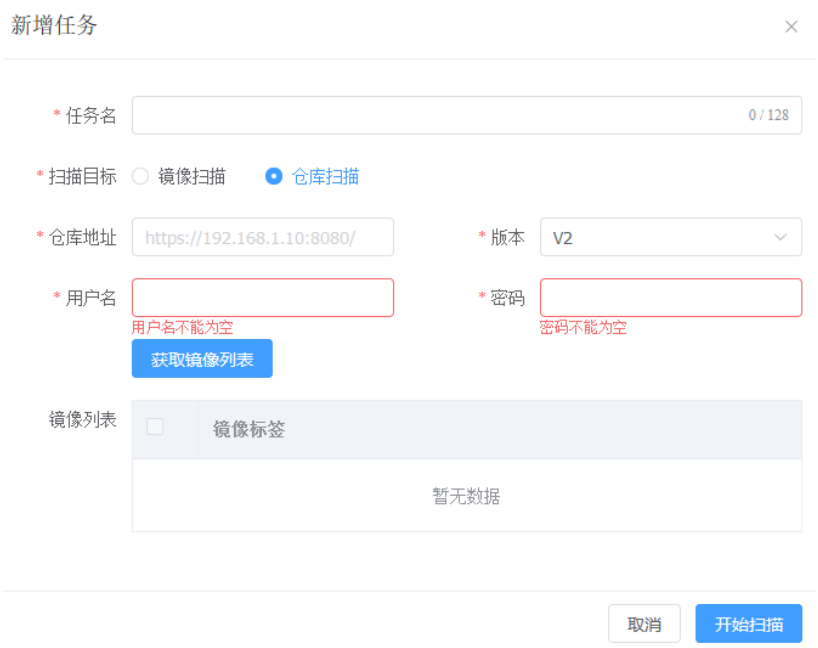
配置项	描述
任务名称	本次创建镜像扫描任务的任务名
扫描目标	镜像扫描：扫描 docker hub 公开仓库中镜像标签进行镜像扫描 仓库扫描：通过登陆 harbor 仓库拉取镜像，选择镜像扫描
仓库类型	公共仓库：docker hub 公开的仓库镜像（无需登陆） 私有仓库：docker hub 个人仓库（需要凭证登陆）
镜像标签	输入扫描目标的镜像标签

扫描目标为 dockerhub 私有仓库扫描如下图：

扫描目标为“dockerhub 私有仓库”参数说明

配置项	描述
任务名称	本次创建镜像扫描任务的任务名
扫描目标	镜像扫描：直接通过镜像标签进行镜像扫描 仓库扫描：通过登陆 harbor 仓库拉取镜像，选择镜像扫描
仓库类型	公共仓库：对外公开的仓库（无需登陆） 私有仓库：dockerhub 私有仓库（需要凭证登陆）
用户名	dockerhub 私有仓库用户名
密码	dockerhub 私有密码
镜像标签	输入扫描目标的镜像标签

扫描目标为仓库扫描如下图：



扫描目标为“仓库扫描”参数说明

配置项	描述
任务名称	本次创建镜像扫描任务的任务名
扫描目标	镜像扫描：直接通过镜像标签进行镜像扫描 仓库扫描：通过登陆 harbor 仓库拉取镜像，选择镜像扫描
仓库地址	仓库访问地址
仓库版本	选择 harbor 仓库对应版本号
仓库用户名	harbor 仓库用户名
仓库密码	harbor 仓库密码
获取镜像列表	点击拉取此仓库下的所有镜像列表
镜像列表	勾选需要扫描的镜像标签

步骤 2. 当任务栏中扫描状态更新为“完成”后，表示扫描任务已完成，可以在任务操作栏中进行扫描结果的查看和其它操作。

镜像扫描任务操作栏说明

操作按钮	描述
	任务信息：查看任务参数信息
	扫描结果：此任务的扫描结果查看
	下载报表：下载此任务扫描结果报表。

	删除：删除此扫描任务。

步骤 3. 镜像扫描任务状态显示完成后，点击操作栏上的结果查看按钮，即可查看此任务结果详情。

6.10 漏洞验证

漏洞本身已经内置了浏览器验证、通用验证功能。但是浏览器验证其实只是对 http response 做了一个渲染，对于一些 xss、link 注入类漏洞验证会比较直观，如果命中的 xss payload 可以弹框的话浏览器验证可以看到弹框的效果。通用验证功能，要人工去修改 http 协议包，这里就需要验证人员了解 http 协议并知道要修改哪块的内容，才能去做验证。对验证人员有一定的要求。

所以我们加入漏洞验证利用功能，主要针对以下几类漏洞：

- SQL 注入：可以直接列出目标的数据库和表。
- 命令执行：可以直接在输入框输入要执行的命令就可以执行任意要执行的命令可以直接一键反弹 shell
- 文件读取：可以直接输入要输入文件路径读取文件。

6.10.1 创建漏洞验证

1. 应用扫描结果中，漏洞列表里，如果此漏洞支持利用验证，可以点击“利用验证”进行漏洞的验证

2. 在[扫描管理]—[应用扫描]—[漏洞验证]页面手动新建利用验证，并查看结果。

★注意：

目前支持的漏洞数据还比较有限，需要逐步迭代。

新建利用验证参数说明

配置项	描述
* Method	请求方法
*URL	目标地址
Header	HTTP 消息头
Body	主体标签信息
*漏洞名称	验证的漏洞选择
漏洞类型	漏洞类型
漏洞描述	漏洞的描述信息
修复建议	漏洞的修复建议信息

7 模板管理

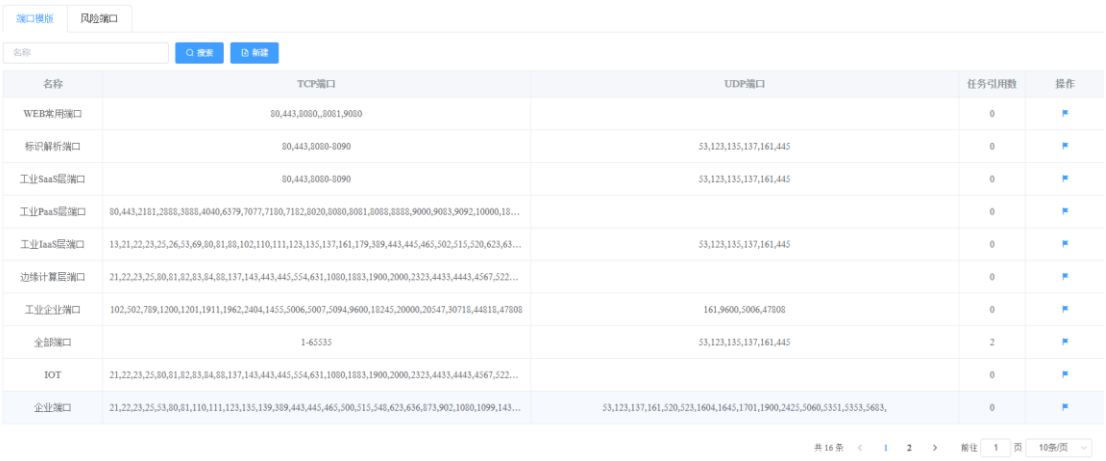
模板管理主要对系统中的各类扫描模板、证书、字典、策略等进行管理，用户通过模板管理可以对所有在任务执行过程中被扫描的内容进行管理

7.1 端口管理

端口管理包含端口模板和风险端口管理配置功能：

- 端口模板：展示了被扫描设备监听端口的端口号、服务类型及其运行协议的相关信息。例： 80 端口对应 http 服务。若在新建扫描任务时配置指定端口扫描模板，那么扫描过程中将只检测端口模板中的端口。系统出厂默认自带 16 种常用端口模板，用户也可自定义端口模板和编辑已有端口模板。
- 风险端口：风险端口开启后，系统扫描任务将会根据开启的风险端口，在【风险管理】—【暴漏端口】中展示所有系统扫描 IP 的风险端口情况，方便管理员快速发现资产存在的风险端口情况。

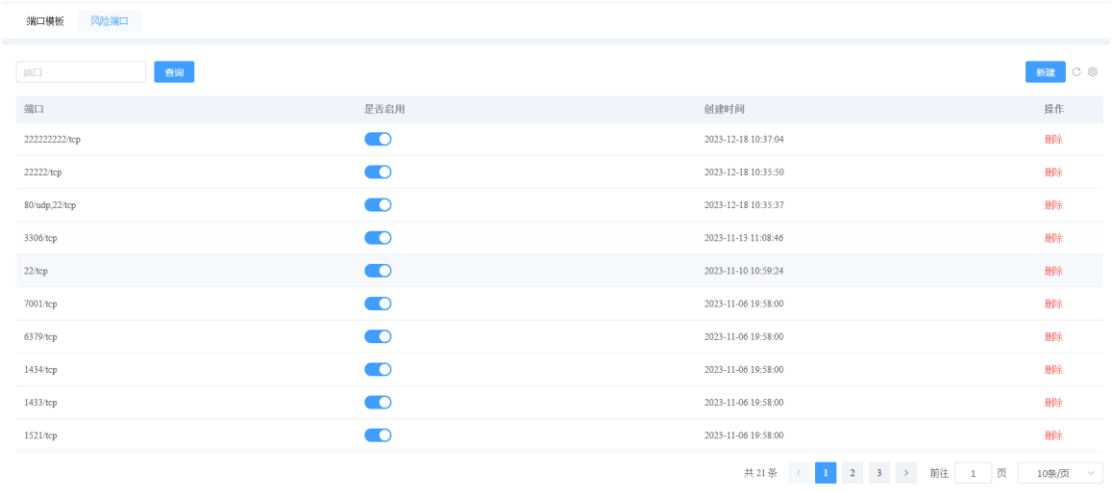
端口模板管理页面说明



端口模板页面参数说明

配置项	描述
名称	端口模板名称
TCP 端口	模板内包含的 TCP 端口号
UDP 端口	模板内包含的 UDP 端口号
任务引用数	当前模板在系统扫描、应用扫描、数据库扫描任务中引用的次数
操作	点击图标后设置为系统扫描、应用扫描、数据库扫描任务中的默认选择模板

风险端口管理列表

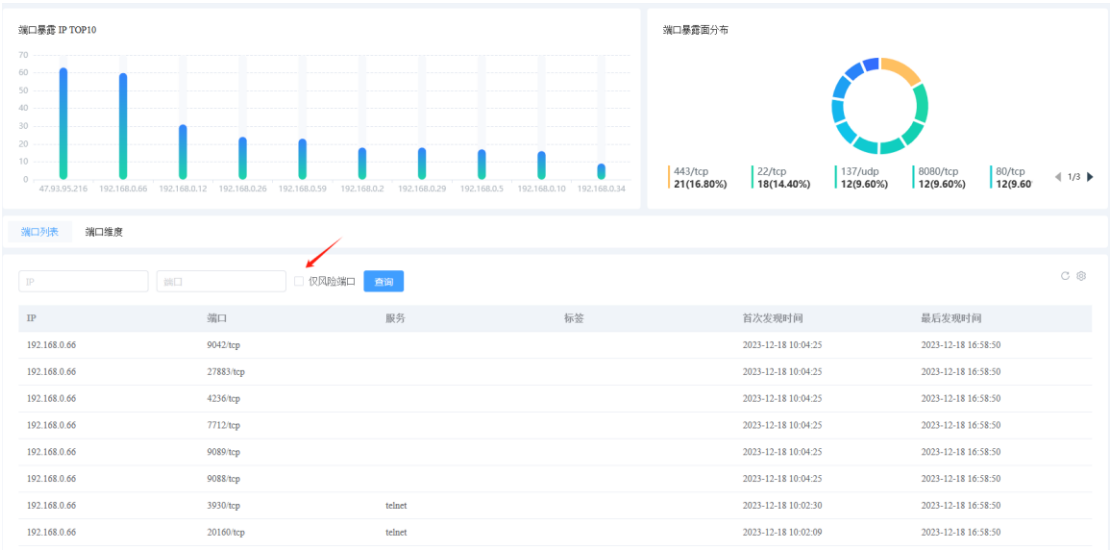


端口模板页面参数说明

配置项	描述
端口	端口号/协议
是否启用	设置是否启用为风险端口
创建时间	风险端口创建时间

操作	点击删除，删除当前风险端口

扫描结果中，在风险管理>暴露端口>勾选风险端口展示列表



7.2 字典管理

在新建口令猜解任务、系统扫描任务的密码爆破以及应用扫描任务中的敏感目录字典选择，需要配置用户名字典、密码字典和敏感目录字典，系统在扫描过程中将根据字典中的内容尝试登录目标设备，若目标设备的登录用户名和密码与密码字典中的内容匹配，则认为目标设备存在脆弱帐号。

字典模式

模式名称	描述
标准模式	用户选择用户名/密码字典进行猜解。
组合模式	用户创建组合字典后，选择组合字典进行猜解

- 进入【模板管理】—【字典管理】，点击“新建”按钮，新建字典。

新建标准模式字典参数说明

配置项	描述

名称	字典名称
字典类型	敏感目录字典：用于应用扫描任务中“敏感目录选择” 用户名字典：密码爆破和口令猜解任务的用户名字典 密码字典：密码爆破和口令猜解任务的密码字典
字典输入	手工输入字典，使用换行分隔
字典上传	上传 txt 文本格式

新建组合模式字典参数说明

配置项	描述
名称	组合模式字典名称
用户名	选择标准模式中创建的用户名字典
密码	选择标准模式中创建的密码字典

字典管理列表操作栏图标说明

图标	描述
下载	下载此字典 txt 文件
编辑	编辑字典，可以重新上传 txt 文本文件
删除	删除字典

7.3 证书管理

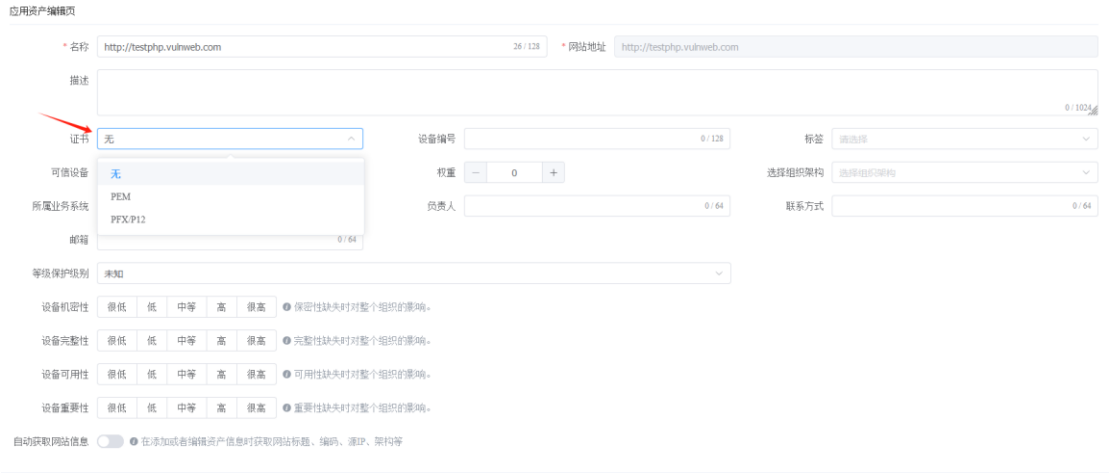
证书管理用于绑定应用资产，可以在应用资产中选择对应的证书，在应用扫描中，可以使用证书访问目标进行扫描，系统支持 PEM 证书、PEM 密钥、PFX/P12。

- 新建证书，点击“新建”按钮，进入新建应用策略模板配置页面。

新建证书参数说明

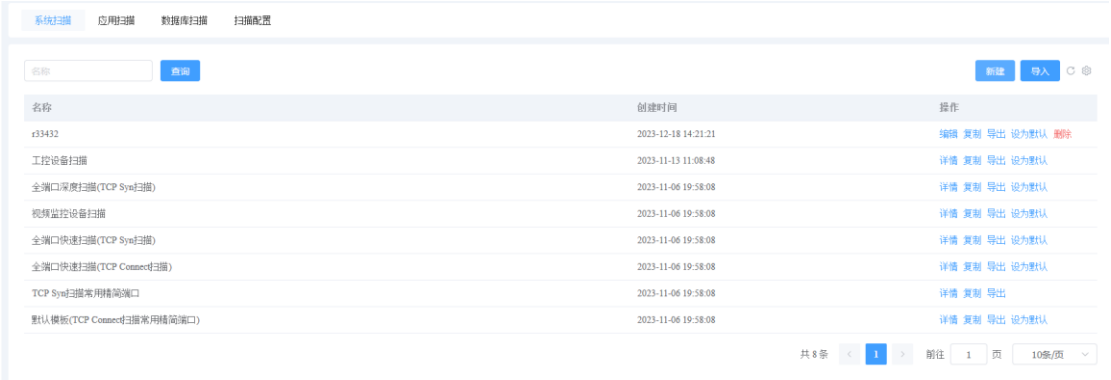
配置项	描述
名称	新建证书名称
证书类型	支持选择 PEM 证书、PEM 密钥、PFX/P12
证书上传	从漏洞库中选择需要的插件，支持通过多种维度对漏洞进行检索

应用资产证书选择页面



7.4 参数模板

参数模板用于对系统扫描、应用扫描、数据库扫描任务的参数进行模板配置，用户可根据不同场景配置相应的扫描参数，提高扫描工作的效率



支持用户配置反连平台

配置项	描述
类型	默认地址、本地地址（推荐）、禁用
IP	反连平台 IP 地址

说明：反连平台用于用于辅助发现无回显命令执行漏洞(如 log4jrce)、SSRF 等漏洞。

7.5 漏洞模板

漏洞模板用于管理系统扫描漏洞模板库、应用扫描漏洞模板库、数据库扫描漏洞模板库：

- 系统扫描漏洞库数大于 300000 条，默认自带 40 多种扫描策略模板，包括：Windows 类系统漏洞、工控类系统漏洞、WEB 漏洞、邮件类系统漏洞等。
- 应用扫描漏洞库数量大于 10000 条，默认自带多种类型扫描策略模板，全面支持对主流 Web 漏洞的识别与扫描，包括：SQL 注入漏洞、命令注入漏洞、CRLF 注入漏洞、LDAP 注入漏洞、XSS 跨站脚本漏洞、路径遍历漏洞等；漏洞规则依据 OWASP 定义的常见 TOP10Web 漏洞进行分类。
- 数据库扫描漏洞库数量大于 4400 条，同时系统默认根据不同类型数据库进行漏洞模板分类。

  所有漏洞都支持通过多种维度对漏洞进行检索，包括：CVE ID、BUGTRAQ ID、CNCVEID、CNVD ID、CNNVD ID、MS 编号、风险等级、漏洞名称、是否使用危险插件、漏洞发布日期等信息，系统扫描策略支持新建和导入。

漏洞模板界面说明

显示项	描述
名称	输入要搜索的扫描策略模板名称
搜索	点击按钮，根据输入的模板名称进行搜索
导入	点击进行导入漏洞模板
新建	点击进入新建漏洞模板界面
模板名称	显示漏洞模板的名称
描述	模板描述
插件个数	当前模板内包含的插件（漏洞）数
任务引用数	当前模板被扫描任务引用次数
操作	导出：导出当前模板，格式为：hostPlugins

- 新建扫描策略模板，点击“新建”按钮，进入新建策略模板配置页面。

新建系统/应用/数据库扫描策略模板参数说明

配置项	描述
模板名称	扫描策略模板名称
描述	模板描述
高级过滤模板	支持将符合筛选的漏洞自动加入自定义漏洞模版
插件	从漏洞库中选择需要的插件，支持通过多种维度对漏洞进行检索

- 导入系统/应用/数据库扫描策略模板，点击“导入”按钮，进入导入策略模板配置页面。

7.5.1 创建系统漏洞模板

用户可以可根据自己需要创建漏洞模板，创建的方法可以通过插件过滤或者高级过滤方式进行漏洞选择

- 插件过滤：通过筛选项过滤，选择符合条件的漏洞并创建模板。
- 高级过滤：通过设置选择条件，如：漏洞名称、危险等级、CVE 编号、漏洞发布时间，满足此条件内的漏洞会自动动态的归类到此模板下。

7.5.2 自定义 POC

针对应用漏洞，除了自带漏洞库以外，系统支持用户手动编写 POC 进行漏洞验证。

7.6 配置模板

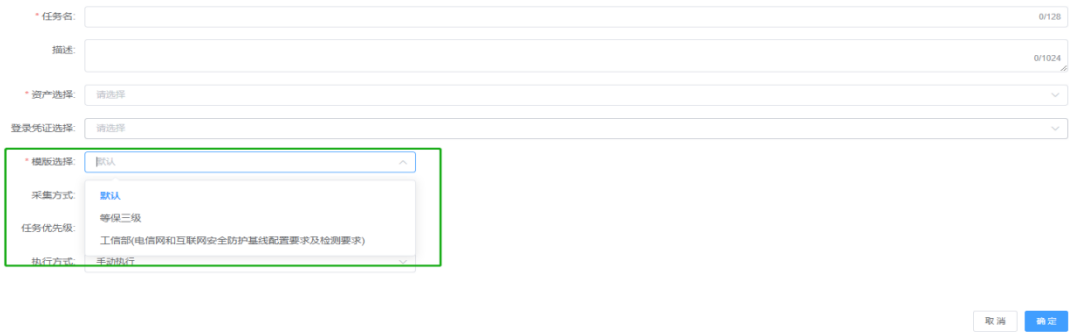
通过不同的配置模板（基线核查策略）可以对目标系统进行自动化的基线检测、分析，方便用户及时发现信息系统中存在的不安全配置，提高目标系统的安全防护水平。系统自带等保三级、工信部(电信网和互联网安全防护基线配置要求及检测要求)等策略，除自带的基线核查策略外，也支持根据用户需求新增基线核查策略。

- 新建基线核查模板，点击“新建”按钮，进入新建基线核查策略模板配置页面。

新建基线核查策略参数说明

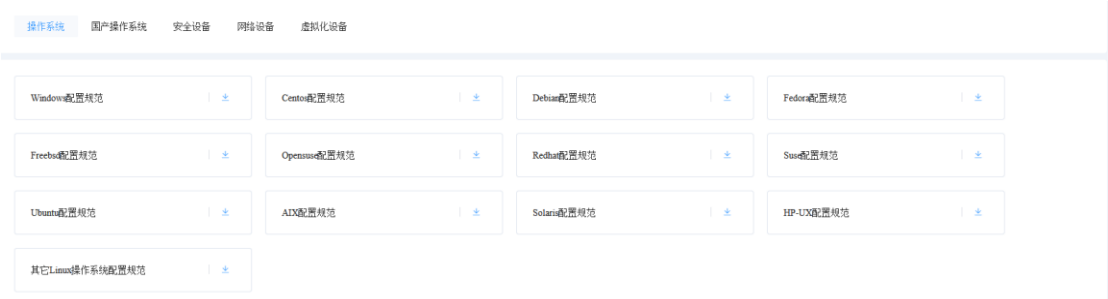
配置项	描述
模板名称	新建基线核查策略名称
插件	从插件库中选择需要的插件，支持通过多种维度对插件进行检索

基线核查任务检查策略选择页面



7.7 离线检查工具

系统提供多种离线检查工具类型，如操作系统、安全设备、网络设备、虚拟化设备，方便用户在离线环境下对目标进行配置核查。



界面参数说明

显示项	描述

工具名称	离线配置核查工具/脚本的名称
下载	下载此工具/脚本到本地

7.8 工控设备信息库

工控设备信息库涵盖了多种工控类型、厂商、型号，用户可以自定义创建，在资产管理网络资产中，可以对工控资产进行指纹选择，系统扫描资产的时候，则优先根据配置的指纹信息进行匹配工控漏洞。

设备类型参数说明

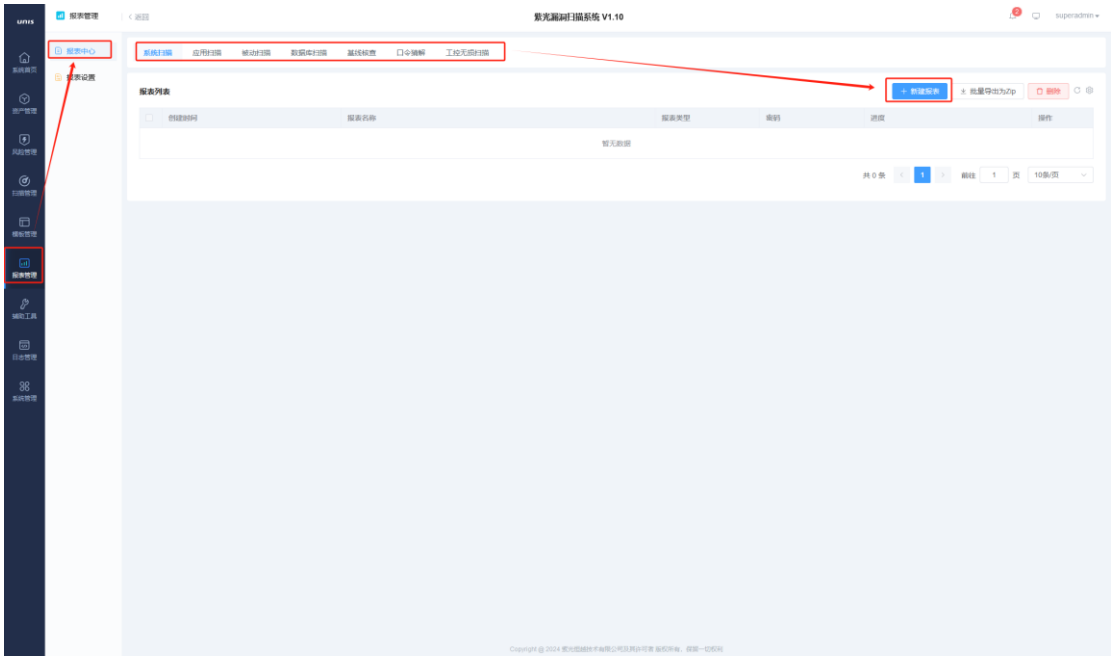
显示项	描述
设备类型 厂商 型号	切换设备类型/厂商/型号管理页面
类型	可输入要搜索的工控类型
搜索	点击进行搜索
新建	新建设备类型
类型	显示设备类型名称
创建时间	显示创建时间
操作	用户新建的可以进行删除操作，默认的则没有删除选项

8 报表管理

报表管理基于系统扫描任务、应用扫描任务、基线核查任务的结果数据，可以预定义、自定义和多角度多层次的分析扫描结果。提供完善的漏洞名称、漏洞编号、漏洞描述、漏洞位置、危险等级、漏洞修复建议。

8.1 系统扫描报表

系统扫描报表基于系统扫描任务的结果数据，用户可以自定义报表名称，选择系统扫描任务、选择生成报表类型（doc、xlsx、html、pdf、xml），可根据漏洞类型过滤生成报表，可以直接预览与下载报表到本地。



系统扫描报表参数说明

配置项	描述
报表名称	默认为：HostScanReport(年月日时分秒)，用户可自定义，报表名称会显示在报表文档中
选择任务	选择要生成报表的系统扫描任务（单选）

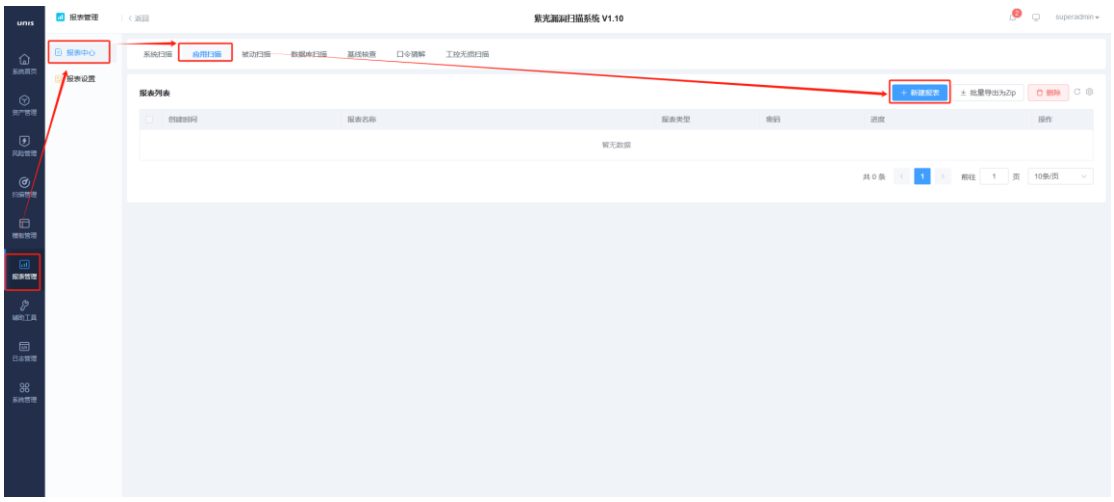
选择资产	选择报表中只显示选择的资产结果数据（默认导出此任务全部资产的扫描结果）
过滤资产	选择生成报表时，过滤任务里指定的资产结果
选择报表类型	可选格式有 html、xlsx、doc、pdf、xml、快测 xml、测评能手 xml
选择漏洞级别	选择指定级别的漏洞在报告中展示详细内容，不影响汇总及统计
密码:	生成报表时进行加密，设置加密密码（支持格式为：html、xlsx、doc）
安全结论:	对报表进行安全结论输入，可生成到报表中（支持格式为：html、pdf、doc）
预览	可直接预览 html 格式的报表
生成报表	点击生成报表，在下方列表中新增一行

系统扫描报表列表图标说明

操作按钮	描述
删除选中	删除选中的任务报表（可批量删除）
批量导出为 ZIP	生成报表数量较多时，支持批量导出到一个 Zip 包中下载到本地
下载	下载此任务报表到本地
删除	删除此报表

8.2 应用扫描报表

应用扫描报表基于应用扫描任务的结果数据，用户可以自定义报表名称，选择系统扫描任务、选择生成报表类型（doc、xlsx、html、xml），可根据漏洞类型过滤生成报表，可以直接预览与下载报表到本地。



应用扫描报表参数说明

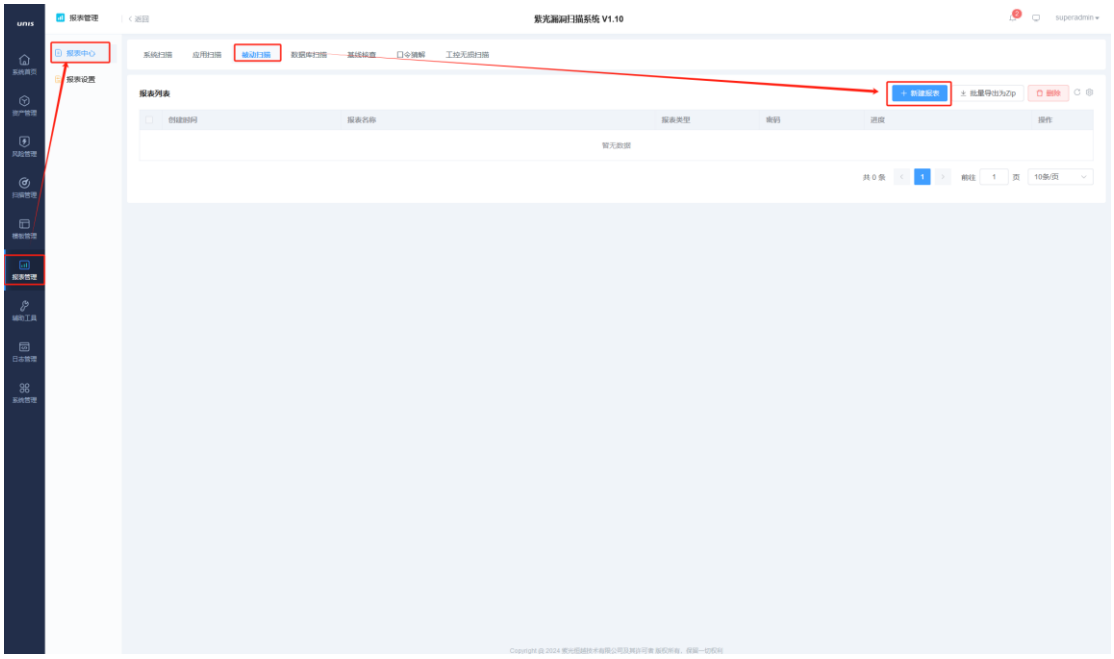
配置项	描述
报表名称	默认为：WebScanReport(年月日时分秒)，用户可自定义，报表名称会显示在报表文档中
选择任务	选择要生成报表的应用扫描任务（单选）
选择资产	选择报表中只显示选择的资产结果数据（默认导出此任务全部资产的扫描结果）
过滤资产	选择生成报表时，过滤任务里指定的资产结果
选择报表类型	可选格式有 html、xlsx、doc、xml、pdf、快测 xml、测评能手 xml
选择漏洞级别	选择指定级别的漏洞在报告中展示详细内容，不影响汇总及统计
密码:	生成报表时进行加密，设置加密密码（支持格式为：html、xlsx、doc）
安全结论:	对报表进行安全结论输入，可生成到报表中（支持格式为：html、pdf、doc）
预览	可直接预览 html 格式的报表
生成报表	点击生成报表，在下方列表中新增一行
导出测试数据包	开启后会把漏洞测试数据导出展示在报表中（漏洞测试数据比较大，会导致报表打开慢，不建议导出）

应用扫描报表列表说明

操作按钮	描述
删除选中	删除选中的任务报表（可批量删除）
批量导出为 ZIP	生成报表数量较多时，支持批量导出到一个 Zip 包中下载到本地
下载	下载此任务报表到本地
删除	删除此报表

8.3 被动扫描报表

被动扫描报表基于被动扫描任务的结果数据，用户可以自定义报表名称，选择被动扫描任务、选择生成报表类型（doc、xlsx、html、xml），可根据漏洞类型过滤生成报表，可以直接预览与下载报表到本地。



被动扫描报表参数说明

配置项	描述
报表名称	默认为：WebScanReport(年月日时分秒)，用户可自定义，报表名称会显示在报表文档中
选择任务	选择要生成报表的被动扫描任务（单选）
选择资产	选择报表中只显示选择的资产结果数据（默认导出此任务全部资产的扫描结果）
过滤资产	选择生成报表时，过滤任务里指定的资产结果
选择报表类型	可选格式有 html、xlsx、doc、xml、pdf、快测 xml、测评能手 xml
选择漏洞级别	选择指定级别的漏洞在报告中展示详细内容，不影响汇总及统计
密码:	生成报表时进行加密，设置加密密码（支持格式为：html、xlsx、doc、pdf）
安全结论:	对报表进行安全结论输入，可生成到报表中（支持格式为：html、pdf、doc）
预览	可直接预览 html 格式的报表
生成报表	点击生成报表，在下方列表中新增一行
导出测试数据包	开启后会把漏洞测试数据导出展示在报表中（漏洞测试数据比较大，会导致报表打

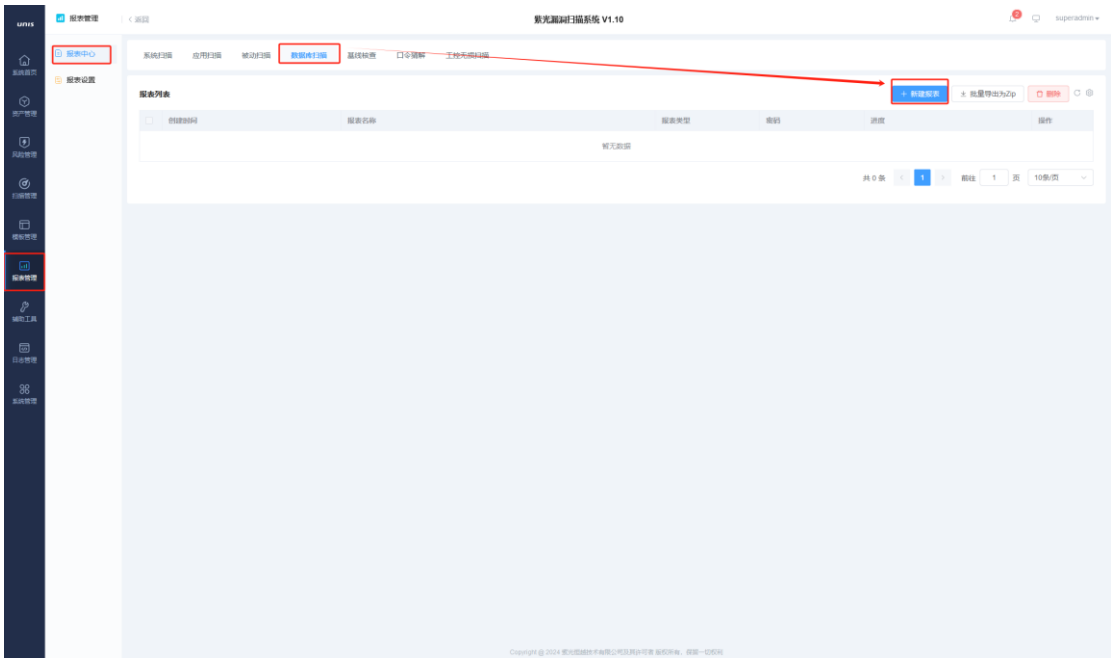
	开慢，不建议导出）

被动扫描报表列表说明

操作按钮	描述
删除选中	删除选中的任务报表（可批量删除）
批量导出为 ZIP	生成报表数量较多时，支持批量导出到一个 Zip 包中下载到本地
下载	下载此任务报表到本地
删除	删除此报表

8.4 数据库扫描报表

数据库扫描报表基于数据库扫描任务的结果数据，用户可以自定义报表名称，选择数据库扫描任务、选择生成报表类型（doc、xlsx、html、pdf、xml），可根据漏洞类型过滤生成报表，可以直接预览或下载报表到本地。



数据库扫描报表参数说明

配置项	描述
报表名称	默认为：DBScanReport(年月日时分秒)，用户可自定义，报表名称会显示在报表文档中

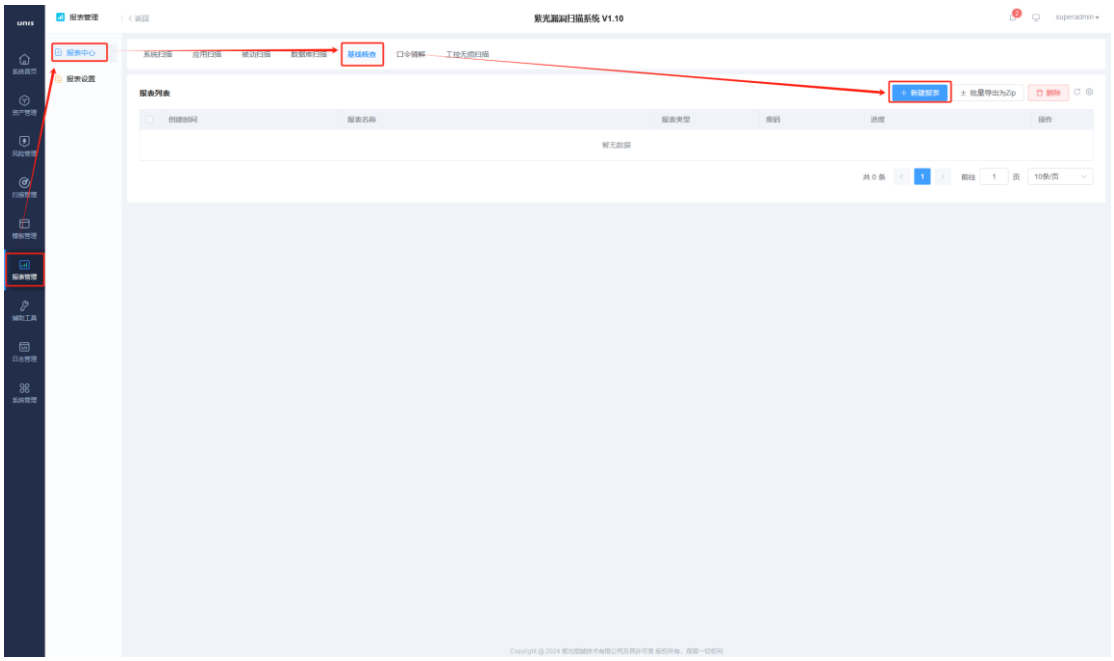
选择任务	选择要生成报表的系统扫描任务（单选）
选择资产	选择报表中只显示选择的资产结果数据（默认导出此任务全部资产的扫描结果）
过滤资产	选择生成报表时，过滤任务里指定的资产结果
选择报表类型	可选格式有 html、xlsx、doc、pdf、xml、快测 xml、测评能手 xml
选择漏洞级别	选择指定级别的漏洞在报告中展示详细内容，不影响汇总及统计
密码:	生成报表时进行加密，设置加密密码（支持格式为：html、xlsx、doc）
安全结论:	对报表进行安全结论输入，可生成到报表中（支持格式为：html、pdf、doc）
预览	可直接预览 html 格式的报表
生成报表	点击生成报表，在下方列表中新增一行

数据库扫描报表列表说明

操作按钮	描述
删除选中	删除选中的任务报表（可批量删除）
批量导出为 ZIP	生成报表数量较多时，支持批量导出到一个 Zip 包中下载到本地
下载	下载此任务报表到本地
删除	删除此报表

8.5 基线核查报表

基线核查报表基于基线核查描任务的结果数据，用户可以自定义报表名称，选择系统扫描任务、选择生成报表类型（doc、xlsx、html、pdf、xml），可以直接预览与下载报表到本地。



基线核查报表参数说明

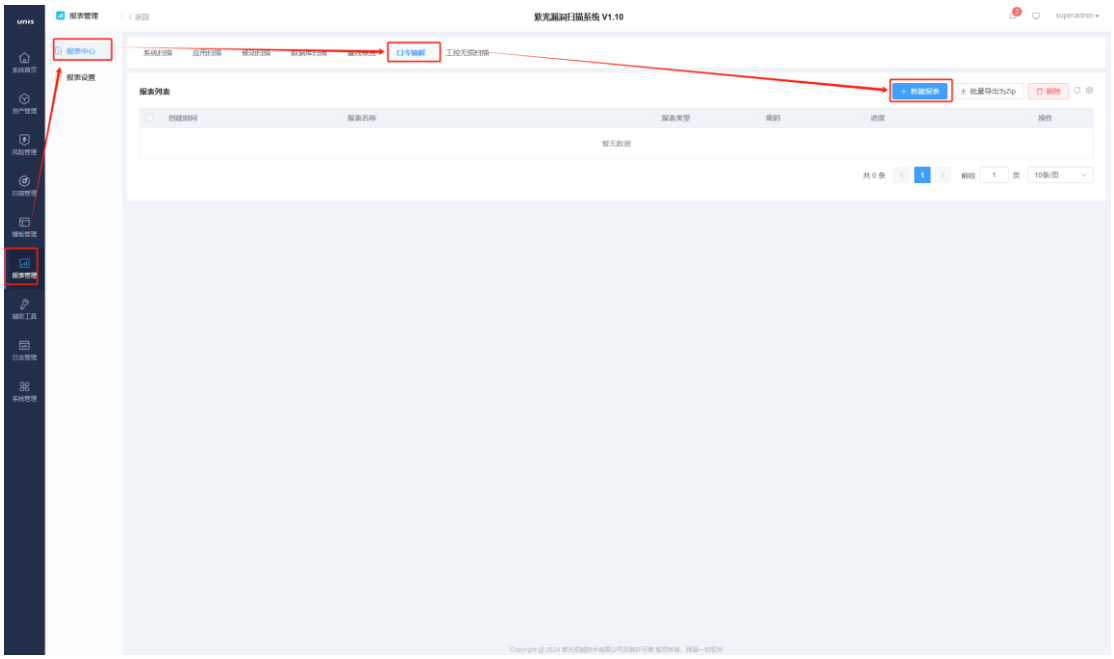
配置项	描述
报表名称	默认为：BenchmarkReport(年月日时分秒)，用户可自定义，报表名称会显示在报表文档中
选择任务	选择要生成报表的应用扫描任务（单选）
选择资产	选择报表中只显示选择的资产结果数据（默认导出此任务全部资产的扫描结果）
过滤资产	选择生成报表时，过滤任务里指定的资产结果
选择报表类型	可选格式有 html、xlsx、doc、pdf、xml
预览	可直接预览 html 格式的报表
生成报表	点击生成报表，在下方列表中新增一行

基线核查报表列表说明

操作按钮	描述
删除选中	删除选中的任务报表（可批量删除）
批量导出为 ZIP	生成报表数量较多时，支持批量导出到一个 Zip 包中下载到本地
下载	下载此任务报表到本地
删除	删除此报表

8.6 口令猜解

口令猜解报表基于口令猜解任务的结果数据，用户可以自定义报表名称，选择口令猜解任务、选择生成报表类型（html、xlsx、pdf），可以直接预览或下载报表到本地。



口令猜解报表参数说明

配置项	描述
报表名称	默认为：BenchmarkReport(年月日时分秒)，用户可自定义，报表名称会显示在报表文档中
选择任务	选择要生成报表的口令猜解描任务（单选）
选择报表类型	可选格式有 html、xlsx、pdf
密码	设置报表密码
自定义安全结论	配置报表安全结论
预览	可直接预览 html 格式的报表
生成报表	点击生成报表，在下方列表中新增一行

口令猜解报表列表说明

操作按钮	描述
删除选中	删除选中的任务报表（可批量删除）

批量导出为 ZIP	生成报表数量较多时，支持批量导出到一个 Zip 包中下载到本地
下载	下载此任务报表到本地
删除	删除此报表

8.7 报表设置

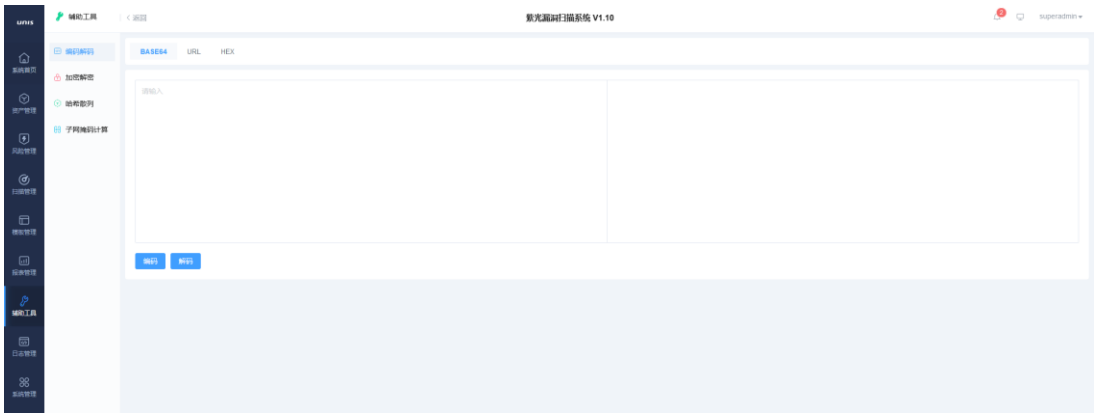
报表设置支持对系统扫描任务、应用扫描任务、数据库扫描任务、基线核查任务、移动扫描任务的 DOC 报表的页眉页脚、logo 进行设置。

报表设置页面参数说明

配置项	描述
页眉	设置 doc 格式报表页眉内容
页脚	设置 doc 报表格式页脚内容
Logo:	点击‘+’上传 logo 图片，格式为 png
保存	保存当前设置
恢复默认	恢复默认设置

9 辅助工具

系统带有 BASE64 编解码、URL 编解码、HEX 编解码；哈希散列加密，包括 DM5、SHA1、SHA224、SHA256、SHA384、SHA512；加解密包括 RC4、AE5。

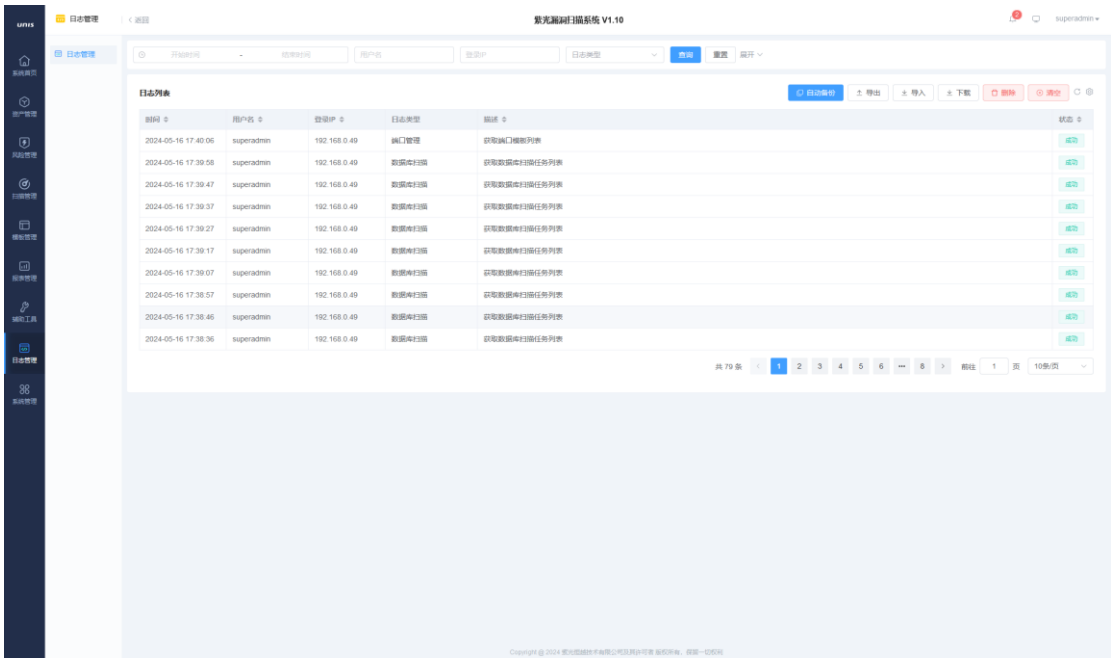


辅助工具页面参数说明

类别	功能	描述
编码解码	BASE64	支持 BASE64 编码方式的编码和解码
	URL	支持 URL 的编码和解码
	HEX	支持 HEX 格式的编码解码
哈希散列	MD5	支持 MD5 加密
	SHA1	支持 SHA1 加密
	SHA224	支持 SHA224 加密
	SHA256	支持 SHA256 加密
	SHA384	支持 SHA384 加密
	SHA512	支持 SHA512 加密
加密解密	RC4	支持 RC4 加密解密
	AE5	支持 AE5 加密解密
子网掩码计算工具		支持根据掩码位数计算主机数

10 日志管理

只有审计管理员 audit 拥有日志管理的权限。系统对用户登录及在设备上的所有操作进行严格审计，并以日志形式输出审计记录，每一条审计日志中包括事件主体、事件发生的时间日期、事件描述和结果等信息。



10.1 查询日志

进入【日志管理】页面，设定查询条件，查看符合查询条件的日志即可。通过查看各类日志信息，系统输出的日志类型主要有以下几种：

- 全部：了解系统的所有情况（包括登录成功、登录失败以及退出登录、任务操作等），及时发现系统全局的操作情况。
- 登陆：了解系统的用户登陆情况（包括登录成功、登录失败以及退出登录、错误锁定等），及时发现未授权用户的尝试登录。
- 登出：了解设备的用户登出情况。

- 网络资产：了解系统的网络资产情况（包括添加资产、获取资产列表以及删除网络资产、更新网络资产等）。
- 应用资产：了解系统的应用资产情况（包括添加资产、获取资产列表以及删除应用资产、更新应用资产等）。
- 组织架构：了解系统的组织架构情况（包括添加部门、获取组织架构以及删除部门等）。
- 凭证管理：了解系统的凭证管理情况（包括添加凭证、获取凭证列表以及删除凭证等）。
- 系统扫描：了解系统的系统扫描任务情况（包括增加系统扫描任务、开始系统扫描任务以及删除系统扫描任务等）。
- 应用扫描：了解系统的应用扫描任务情况（包括增加应用扫描任务、开始应用扫描任务以及删除应用扫描任务等）。
- 基线核查：了解系统的基线核查任务情况（包括增加基线核查任务、开始基线核查任务以及删除基线核查任务等）。

10.2 其它操作

日志管理支持日志导入、导出（备份）、删除、清空等操作

操作按钮	描述
导出	对日志进行导出备份，可以指定导出多少日以内的日志，输入 0 则导出全部日志
导入	导入 logback 后缀格式的文件日志
下载	下载指定日期时间段的日志到本地
删除	删除指定的日志记录
清空	清空所有日志记录
自动备份	选择备份方式，支持邮件发送和 FTP 同步两种方式，支持自定义设置备份周期

11 系统管理

只有系统管理员 admin 拥有系统管理的权限，包括用户管理、角色管理、引擎管理、告警配置、设备管理、诊断工具、升级管理、系统管理、关于等。

11.1 用户管理

用户管理支持查看默认用户信息、新建用户、账号解锁等操作，支持与 AD 域、Radius 或其他遵循 LDAP 协议的第三方认证系统的集成。

系统用户采用三权分立设计原则，分为管理员、审计员和安全员，用户信息如下：

角色	初始账号/密码	说明
管理员	admin/admin@123	可以进行系统管理、用户设置等
安全员	user/user@123	扫描功能模块使用
审计员	audit/audit@123	日志审计查询
超级管理员	superadmin/superadmin@123	所有权限

用户管理界面参数说明

配置项	描述
搜索	根据输入的用户名信息进行筛选展示
新建	新建用户
登录IP	查看访问系统的 IP 记录，支持对锁定 IP 进行解锁操作
LDAP同步	配置 LDAP 协议认证集成
会话管理	查看系统当前交互会话，管理员可以进行删除会话，删除后需要用户重新登陆
用户名	用户名名称
所属角色	所属角色名称
姓名	用户名的姓名信息
邮箱	用户名的邮箱信息
是否被锁定	用户是否被锁定
来源	用户来源（默认/LDAP）
操作	编辑:编辑用户信息 重置双因素认证：重置用户双因素认证信息 解锁:解锁当前用户 删除：删除用户

LADP 同步说明

配置项	描述
是否启用	勾选则启用同步，不勾选则不启用（启用后每个整点会同步一次用户列表）
IP	AD 域服务器 IP
端口	默认：389
Base DN	域目录分区名
用户筛选规则	默认填写：(&(objectCategory=Person)(sAMAccountName=%s))
用户属性	默认填写：sAMAccountName
用户名	用户名
密码	用户密码
测试连接	测试是否可连接域
立即同步用户	点击立即将此域分区下的用户信息同步至漏扫系统

保存	保存配置

- 新建用户：在【系统管理】—【用户管理】中，点击“新建”按钮，进入新建用户页：

新建用户参数说明

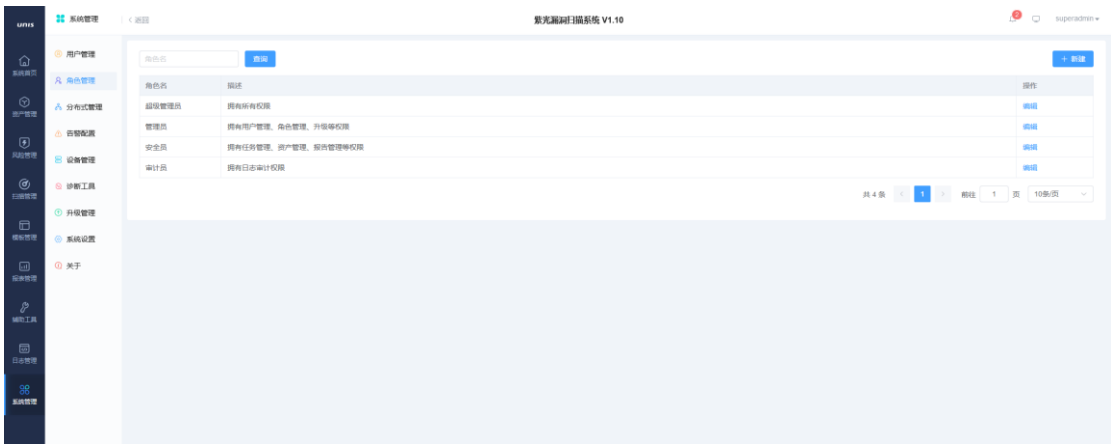
配置项	描述
用户名	新建用户用户名（等同于登录名）
密码	用户的登陆密码（密码长度最小 12 位，密码至少包含数字、大写、小写、特殊字符中 3 种。）
所属角色	用户所属角色（在“角色管理”中可新建）
姓名	使用者姓名
邮箱	使用者邮箱号
账号到期时间	设置此用户的有效期，为空则表示永不过期
扫描目标类型	● 白名单：选择白名单后，代表对扫描目标框设置的目标进行扫描 ● 黑名单：选择黑名单后，代表不可以扫描目标框设置的目标进行扫描
扫描目标	192.168.1.1,192.168.1.0/24。仅支持 IP 和掩码方式,多个用逗号分割!为空时表示所有 IP 段均可访问
最大扫描 IP 数:	设置当前用户最大可扫描的 IP 数
最大扫描域名数:	设置当前用户最大可扫描的域名数

用户管理列表操作栏说明

操作按钮	描述
	按钮打开表示此用户已被锁定
编辑	编辑此用户信息
重置双因素认证	重置此用户双因素认证
解锁	当用户被锁定后，进行解锁操作

11.2 角色管理

系统角色采用三权分立设计原则，分为管理员、审计员和安全员，管理员可以根据实际情况新建角色。



角色	权限说明
管理员	拥有用户管理、角色管理、升级等权限
安全员	拥有任务管理、资产管理、报告管理等权限
审计员	拥有日志审计管理权限

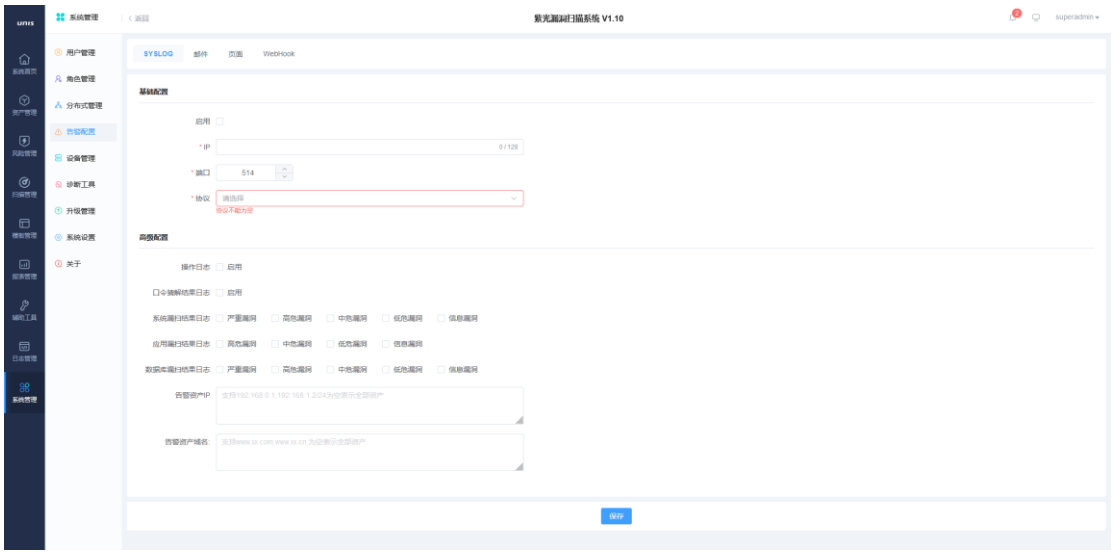
- 新建角色：在【系统管理】—【角色管理】中，点击“新建”按钮，进入新建角色页：

新建角色参数说明

配置项	描述
角色名	新建角色角色名称
描述	角色描述
权限	分配角色权限（可选系统首页、资产管理风险管理、风险检测、模板管理、报表管理、辅助工具、日志管理、系统管理等菜单及子菜单功能权限）

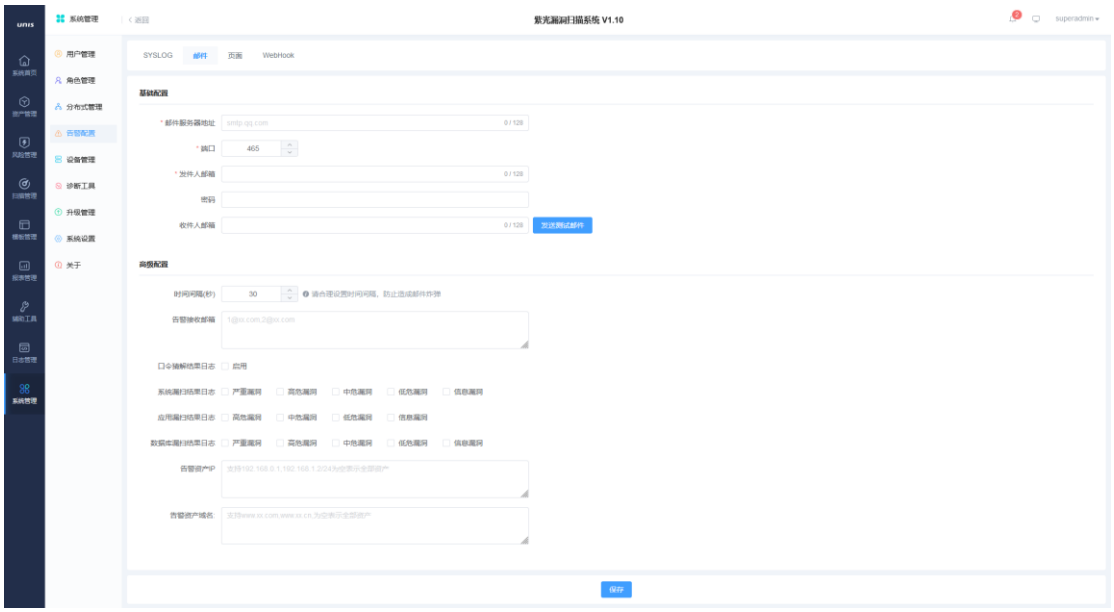
11.3 告警配置

系统告警配置支持以 syslog 转发、邮件、页面方式进行告警。



syslog 启用配置参数说明

配置项	描述
启用	启用或关闭
IP	发送接收 IP
端口	传输端口号（默认 514）
协议	传输协议（TCP/UDP）
操作日志	是否发送操作日志
口令猜解结果日志	是否发送口令猜解结果日志
系统漏扫结果日志	勾选对应漏洞等级的漏洞，勾选后将进行告警
应用漏扫结果日志	勾选对应漏洞等级的漏洞，勾选后将进行告警
数据库漏扫结果日志	勾选对应漏洞等级的漏洞，勾选后将进行告警
告警资产 IP	设置告警的资产 IP，支持 192.168.0.1,192.168.1.2/24 为空表示全部资产
告警资产域名	设置告警的资产域名，支持 www.xx.com,www.xx.cn,为空表示全部资产



告警邮件配置参数说明

配置项	描述
邮件服务器地址	邮件服务器的 IP 地址（地址可以是 IP 地址，也可以是域名）
端口	协议端口号
发件人邮箱	发件人邮箱号
密码	发件人邮箱密码
收件人邮箱	收件人邮箱号
发送测试邮件	发送一封测试邮件，验证邮件配置是否正常
时间间隔（秒）	设置邮箱发送间隔时间（请合理设置时间间隔，防止造成邮件炸弹）
告警接收邮箱	设置告警接收邮箱
操作日志	是否发送操作日志
口令猜解结果日志	是否发送口令猜解结果日志
系统漏扫结果日志	勾选对应漏洞等级的漏洞，勾选后将进行告警
应用漏扫结果日志	勾选对应漏洞等级的漏洞，勾选后将进行告警
数据库漏扫结果日志	勾选对应漏洞等级的漏洞，勾选后将进行告警
告警资产 IP	设置告警的资产 IP，支持 192.168.0.1,192.168.1.2/24 为空表示全部资产
告警资产域名	设置告警的资产域名，支持 www.xx.com,www.xx.cn,为空表示全部资产

页面告警配置参数说明

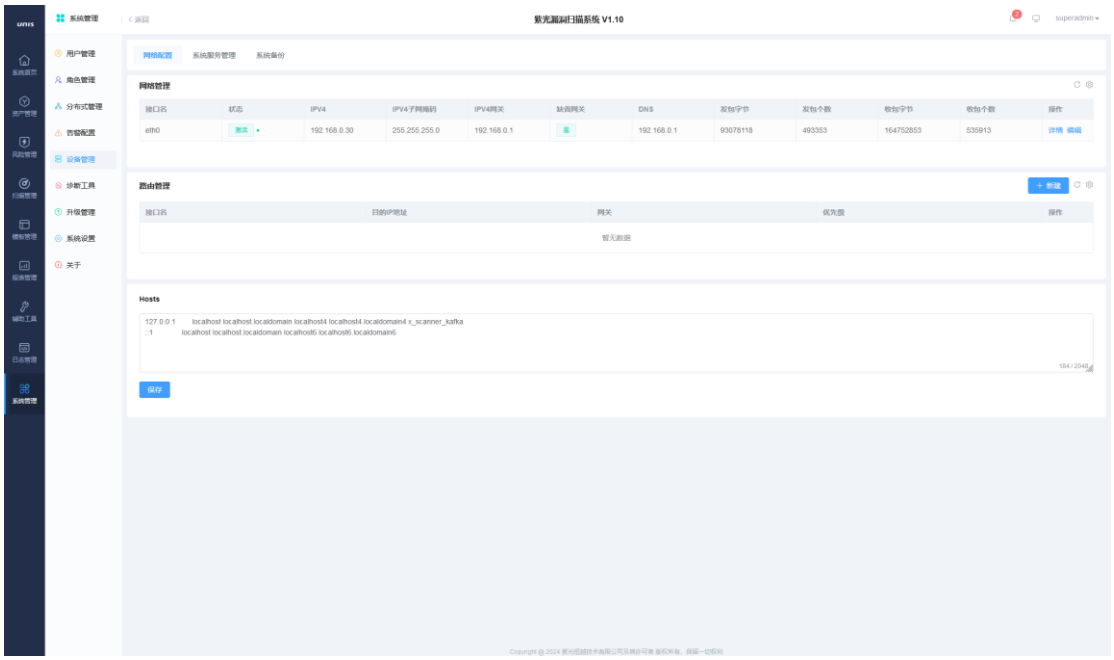
配置项	描述
操作日志	是否发送操作日志
口令猜解结果日志	是否发送口令猜解结果日志
系统漏扫结果日志	勾选对应漏洞等级的漏洞，勾选后将进行告警
应用漏扫结果日志	勾选对应漏洞等级的漏洞，勾选后将进行告警
数据库漏扫结果日志	勾选对应漏洞等级的漏洞，勾选后将进行告警
告警资产 IP	设置告警的资产 IP，支持 192.168.0.1,192.168.1.2/24 为空表示全部资产
告警资产域名	设置告警的资产域名，支持 www.xx.com,www.xx.cn,为空表示全部资产

11.5 设备管理

设备管理包括网络管理、DNS 配置、Hosts 配置、时间同步、服务管理等配置管理，本节将分别予以详细介绍。

11.5.1 网络配置

在网络管理功能模块，系统管理员可以对系统设备的各个网络扫描接口进行管理和配置 DNS 服务器、Hosts 配置。所谓网络扫描接口，就是设备用于与其他设备交换扫描结果数据并相互作用的部分，其功能就是完成设备之间的数据交换。物理接口真实存在、有相应的硬件支持，如 UNIS X1000-12T12F-G2 设备支持的 eth0、eth1、eth2、eth3、eth4、eth5。



11.5.1.1 网络管理

进入【系统管理】—【设备管理】中的网络管理，点击指定接口的编辑按钮，进入编辑接口信息

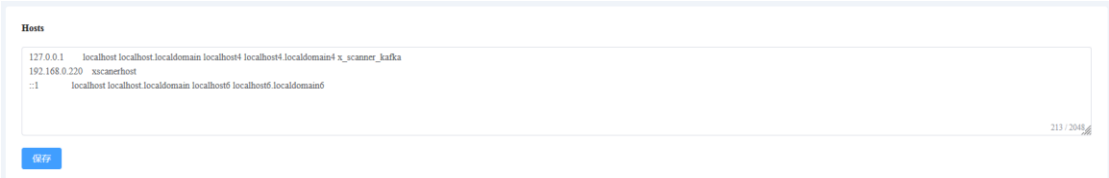
接口信息配置参数说明

配置项	描述
接口名	接口名称，无法修改
IPV4 类型	选择 IPV4 网络配置类型（DHCP、Static）
Ipv4	配置 IPV4 地址
IPV4 子网掩码	配置子网掩码
IPV4 网关	配置 IPV4 网关地址
IPV4 DNS	配置 DNS 服务器地址
IPV6 类型	选择 IPV6 网络配置类型（DHCP、Static）
IPV6	设置 IPV6 地址
IPV6 网关	设置 IPV6 网关
缺省网关	设置此接口是否为缺省网关

注：若需系统进行在线升级，网关和 DNS 服务器必须正确配置

11.5.1.2 Hosts 配置

配置 IP 域名的映射关系，填写的时候 IP 地址要放在前面，空格后再写上映射的 Host name(主机名)，注意默认的不要去删除。



11.5.1.3 路由管理

路由管理可新建、删除管理系统路由。

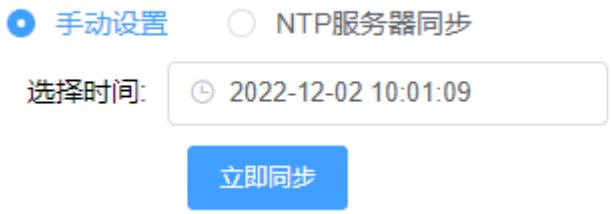
新建路由

11.5.2 系统服务管理

11.5.2.1 时间同步

时间同步能够对系统时间进行配置，有以下两种方式：

手动设置



NTP 服务器同步

11.5.2.2 服务管理

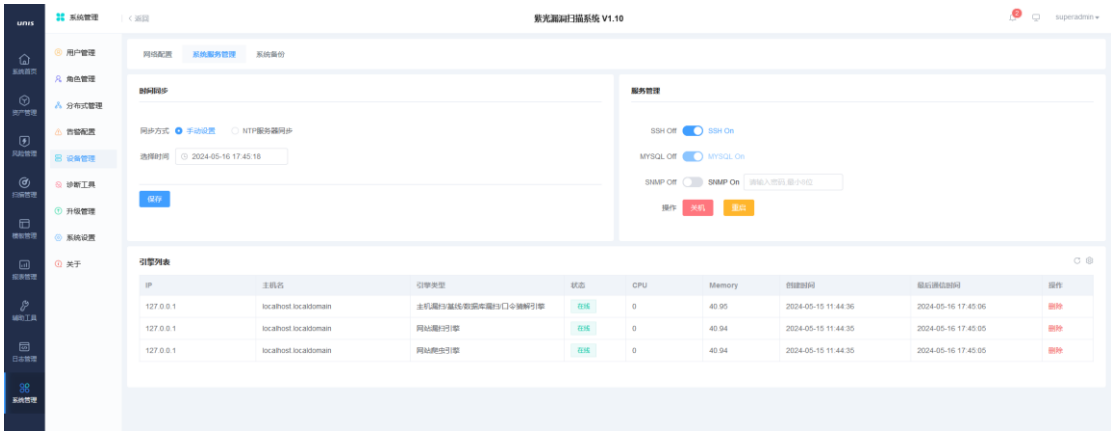
服务管理支持对系统进行关机、重启、SSH 服务、SNMP 服务打开/关闭等操作

服务管理图标说明

图标	描述
× 关机	对系统进行关机操作
重启	对系统进行重启操作
SSH Off SSH On	打开或关闭 SSH 服务
SNMP Off SNMP On	打开或关闭 SNMP 服务以及设置密码

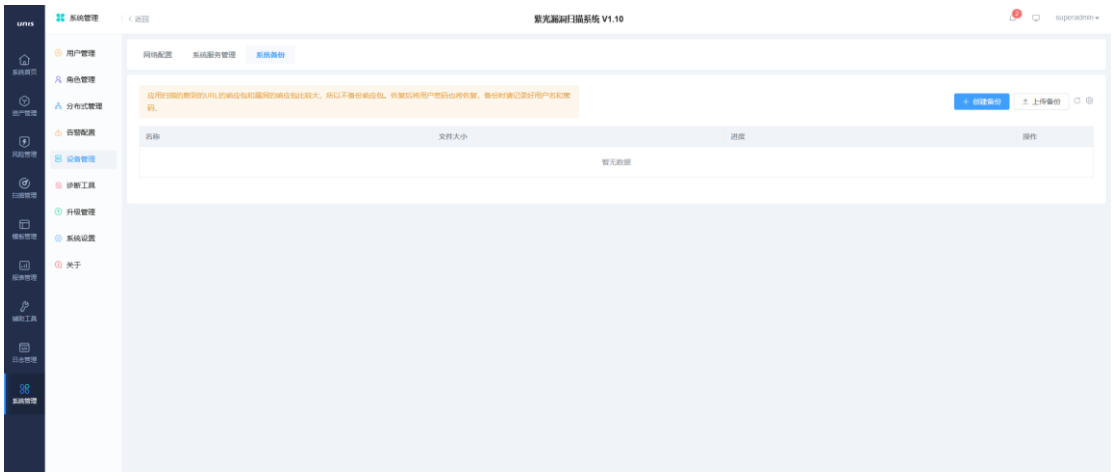
11.5.2.3 引擎列表

查看系统引擎在线情况以及运行状态，包括网站漏扫引擎、爬虫引擎、主机漏扫引擎。如果是离线说明有异常，无法正常进行任务扫描。



11.5.3 系统备份

系统提供对资产数据、扫描任务数据、用户数据进行备份恢复。



★注意：

1. 应用扫描的爬到的 URL 的响应包和漏洞的响应包比较大，所以不备份响应包。
2. 还原后将用户密码也将还原，备份时请记录好用户名和密码。

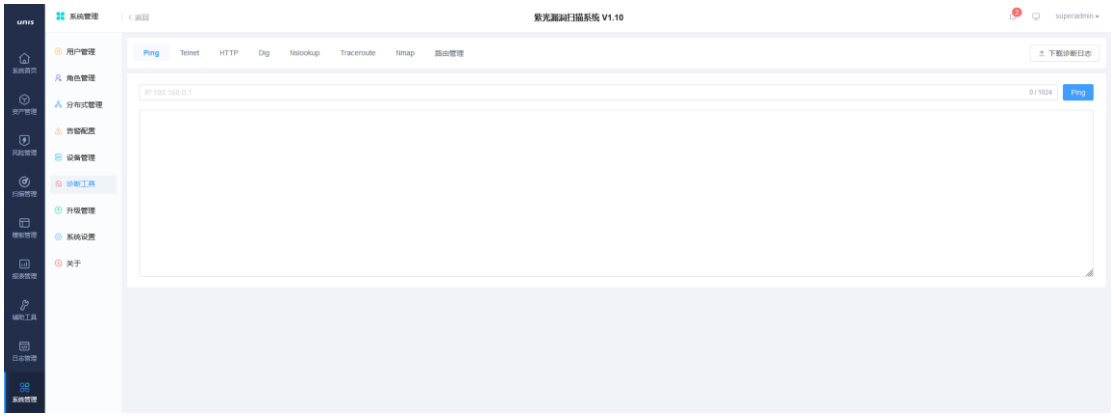
参数说明

名称	描述

创建备份	对当前时间点数据进行备份
上传备份	上传备份文件
名称	备份文件名称
文件大小	备份文件大小
进度	备份进度
操作	下载：下载备份文件到本地 还原：指定备份文件进行还原操作（恢复后将用户密码也将恢复，备份时请记录好用户名和密码） 删除：删除备份文件

11.6 诊断工具

诊断工具提供常用工具用于设备的诊断和排错，本节介绍常用工具的使用方法。进入【系统管理】【诊断工具】，即可使用常用工具。



- **Ping**: Ping 命令用于检测设备存活或与网络中其他设备的连接情况，帮助分析、判定网络故障。在文本框中输入 IPv4 地址、IPv6 地址或主机名，单击【Ping】按钮，稍后可见执行结果。
- **Telnet**: Telnet 是 Internet 远程登录服务的标准协议和主要方式，使用此工具可以查看目标设备的 Telnet 服务是否开启，在文本框中输入 IPv4 地址、IPv6 地址或主机名，单击【telnet】按钮，稍后可见执行结果。
- **HTTP**:HTTP 工具模拟真实的 Get 请求，获取网页完整源码，用此工具可以查看能否正常访问目标域名，在文本框中输入 URL 地址，单击【HTTP】按钮，稍后可见执行结果。
- **DIG**:是常用的域名查询工具，可以从 DNS 域名服务器查询主机地址信息，获

取到详细的域名信息，点击【dig】按钮，稍后可见执行结果。

- Nslookup:查询域名信息的一个非常有用的命令，可以指定查询的类型，可以查到DNS记录的生存时间还可以指定使用哪个DNS服务器进行解释,在文本框中输入域名地址，点击【Nslookup】按钮，稍后可见执行结果。
- Traceroute:命令利用 ICMP 协议定位您的计算机和目标计算机之间的所有路由器，在文本框中输入域名或者 IP，点击【Traceroute】按钮，稍后可见执行结果。
- **诊断日志：**诊断日志主要用于系统故障排查，当系统出现使用问题，可下载诊断日志发给厂家研发排查。

11.7 升级管理

升级管理包括软件升级和漏洞库升级。

11.7.1 软件升级

- **离线升级：**当系统无法正常连接到升级服务器时，通常需要管理员手动升级设备：

  进入【系统管理】—【升级管理】软件升级，点击“离线升级”按钮，进入离线升级包上传页面，点击“上传文件”,选择本地的升级包（dat文件）进行上传，当提示“上传成功”后，再点击“确定升级”按钮进行升级，当提示“升级成功，请等待几秒后刷新页面”后，等待 10 秒左右刷新页面，即可升级成功，在升级历史中也会新增一条升级记录。

时间	升级前版本	升级后版本	升级说明
2022-12-02 10:57:27	3.0.0.60	3.0.0.64	1、功能优化

11.7.2 漏洞库升级

- **离线升级：**当系统无法正常连接到升级服务器时，通常需要管理员手动升级设备：

  进入【系统管理】—【升级管理】漏洞库升级，点击“离线升级”按钮，进入离线升级包上传页面，点击“上传文件”,选择本地的升级包（dat

文件）进行上传，当提示“上传成功”后，再点击“确定升级”按钮进行升级，当提示“升级成功，请等待几秒后刷新页面”后，等待 10 秒左右刷新页面，即可升级成功，在升级历史中也会新增一条升级记录。

★注意:

升级前请先停止所有扫描任务,升级完成后服务将自动重启，刷新页面即可。

时间	升级前版本	升级后版本	升级说明
2022-12-02 10:57:27	3.0.0.60	3.0.0.64	1、功能优化

- **自动升级:**若需系统进行漏洞库在线升级,网关和 DNS 服务器必须正确配置，当系统可以与漏洞库升级服务器互通时，系统会自动检测本地漏洞库版本是否为最新版本，如果不是，则会自动下载最新漏洞库版本到本地缓存，用户需进入【系统管理】—【升级管理】漏洞库升级，点击“检查新版本”按钮后，在弹出的对话框，点击“确定升级”后，系统进行漏洞库升级；同时支持自动定时升级，可以设置每天、每周、每月。

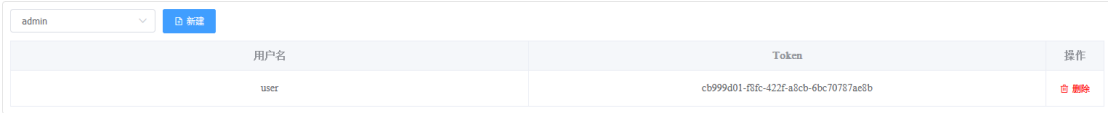
11.8 系统设置

系统设置主要包含 API Key 设置、WSUS 设置、磁盘使用监控设置、双因素认证设置、系统设置等。

11.8.1 API Key 设置

系统具备标准开放的接口，通过生成的 API Key，，可为其他类型安全产品编写相应的程序模块，达到与 UNIS X1000-12T12F-G2 系统进行联动的目的。

- 选择对接的用户
- 点击“新建”按钮后，系统会生成 API Key:



11.8.2 WSUS 设置

WSUS（Windows Server Update Services）是微软公司推出的网络化的补丁分发方案，WSUS 支持微软全部产品的更新，包括 Office、SQL Server 等内容。

内部网络中设置 WSUS 后，所有 Windows 更新都集中下载到内部网的 WSUS 服务器中，网络中的目标主机通过 WSUS 服务器即可得到更新。既节省了网络资源，避免了外部网络流量浪费，又提高了内网主机更新的效率。

WSUS 服务器参数说明

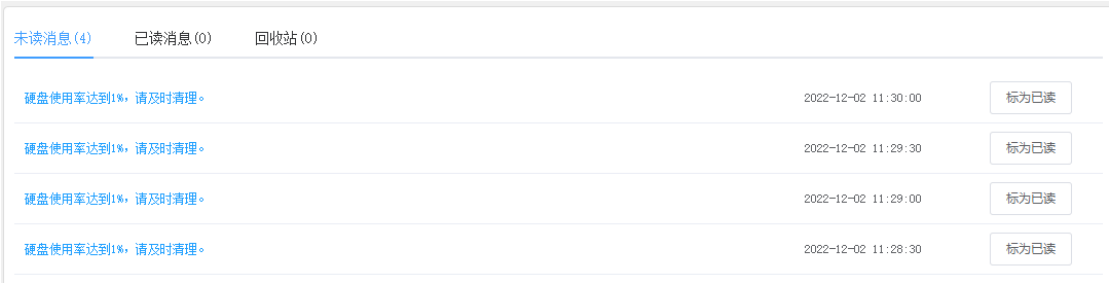
配置项	描述
WSUS IP	WSUS 服务器的 IP 地址
安装方式	导入 WSUS 联动配置文件之后，升级包的安装方式。 提醒：导入 WSUS 联动配置文件之后，提醒用户是否立即安装升级包 不提醒：导入 WSUS 联动配置文件之后，直接安装。

11.8.3 磁盘使用监控设置

磁盘中存储的数据达到磁盘状态告警配置中设置的百分比，系统将发出告警，通知管理员。

进入 【系统管理】 —【系统设置】 页面，在“磁盘使用监控”区域，配置告警百分比即可，系统默认值为 30%。

系统提示如下：



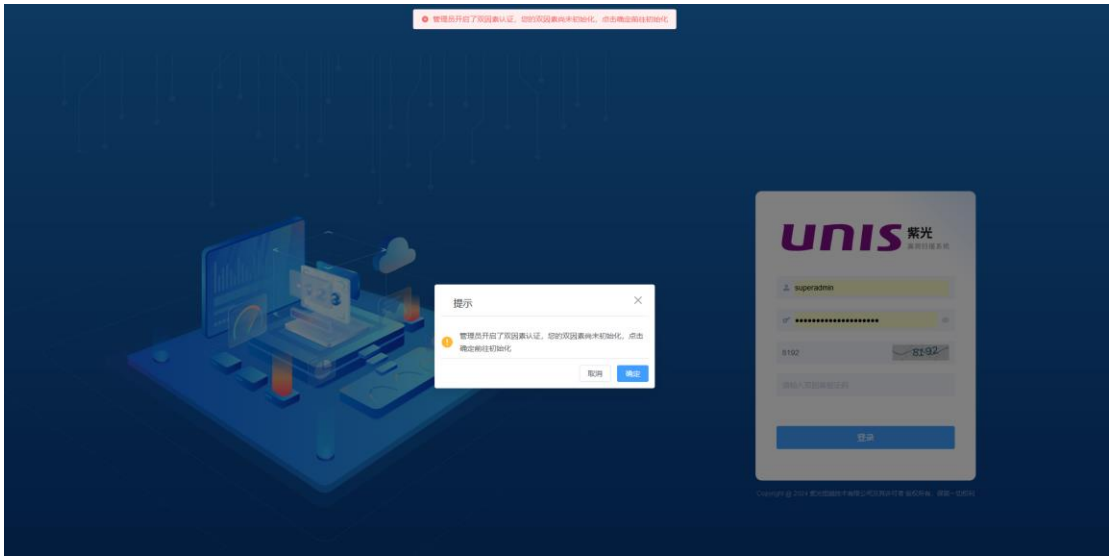
11.8.4 双因素认证设置

双因素认证是一种采用时间同步技术的系统，采用了基于时间、事件和密钥三变量而产生的一次性密码来代替传统的静态密码。每个动态密码卡都有一个唯一的密钥，该密钥同时存放在服务器端，每次认证时动态密码卡与服务器分别根据同样的密钥，同样的随机参数（时间、事件）和同样的算法计算了认证的动态密码，从而确保密码的一致性，从而实现了用户的认证。解决因口令欺诈而导致的重大损失，防止恶意入侵者或人为破坏，解决由口令泄密导致的入侵问题。

- 点击【系统管理】--【系统设置】--【双因素认证】开关开启/关闭，即可启用或者停用双因素认证。

双因素认证登陆，输入用户名/密码以及验证码，点击登陆，第一次需要初始化，如下图：

初始化：



提示需要下载工具进行扫描，点击下载：

下载后，需要使用手机安装 apk 应用，然后打开 apk 进行扫描双因素认证二维码，然后生成双因素验证码即可进行绑定登陆。

★注意：

令牌应用可在系统商店下载，安卓系统应用名称为：Google 身份验证器；ios 系统应用名称为：Authenticator。

11.8.5 密码策略

密码策略设置对用户的密码复杂的进行配置

密码策略配置说明

配置项	描述
最小长度	设置用户密码的最小长度值
密码复杂度	开启后，密码至少包含数字、大写、小写、特殊字符中 3 种。
密码最长使用天数	0 表示永久，否则到期必须修改密码

11.8.6 系统设置

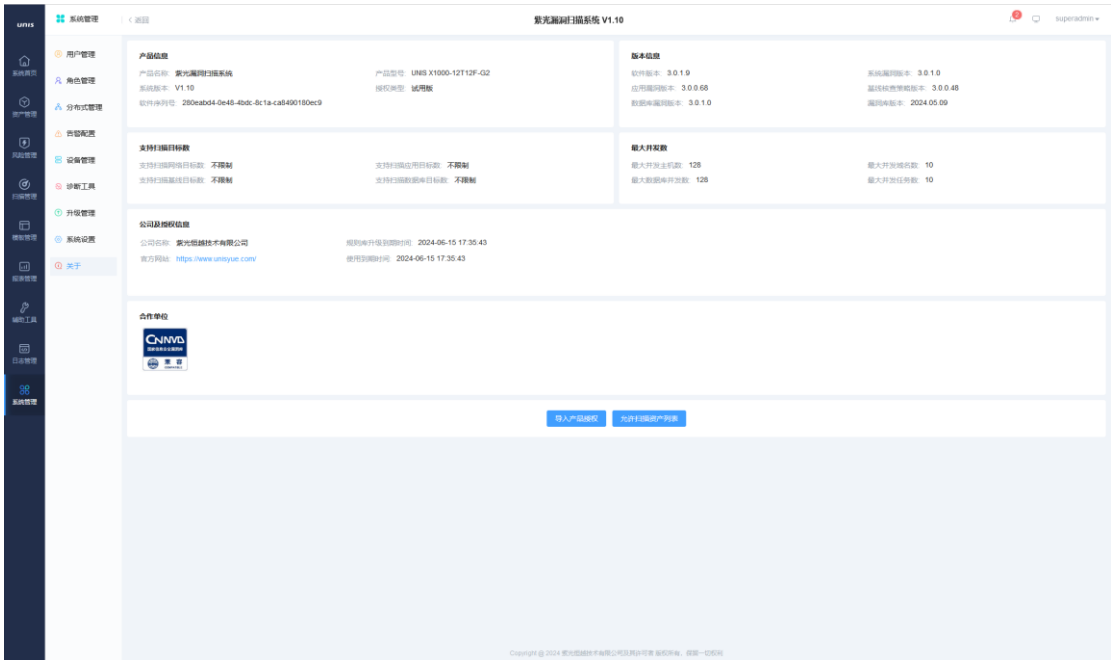
为了保证系统安全性，防止恶意的多次尝试密码登录，系统设置了登录失败锁定功能、登录超时退出、允许登录的 IP/段、管理员可以设置允许的最大登录重试次数、超过最大重试次数后的处理方法，并且可以解锁被锁定的 IP 或帐号。

系统设置参数说明

配置项	描述
登陆验证码	选择开启/关闭登陆验证码
连续登陆失败锁定方式	1. 锁定用户名 2. 锁定登陆 IP
登录超时退出时间	设置系统登录超时退出时间（秒），默认值为 1800，可选值 1～99999
最大允许失败次数	设置系统允许的最大登录重试次数，默认值为 5，可选值为 1～99999
账号锁定时间	设定帐号的锁定时间，默认为 300 秒。仅当“超过最大允许失败次数”选择锁定锁定帐号时该参数配置生效。
允许登录 IP/段（白名单）	设置允许登录系统的 IP/段，支持 IP 和掩码方式，为空时表示所有 IP 网段都可访问。
允许登录 IP/段（黑名单）	设置不允许登录系统的 IP/段，支持 IP 和掩码方式，为空时表示所有 IP 网段都可访问。

11.9 关于

关于信息里面包含系统信息查看，包括系统最大并发数、系统漏洞版本等信息，以及产品使用到期时间和激活产品授权等内容



关于信息说明

参数项	说明
产品名称	当前产品名称

产品型号	当前产品型号
系统版本	当前产品系统版本号
软件版本	当前产品软件版本号
漏洞库版本	当前产品漏洞版本号
授权类型	当前产品授权类型
软件序列号	当前产品软件序列号
最大并发任务数	当前产品同一时间内系统支持执行扫描任务的最大数目
系统漏洞版本	当前产品系统漏洞版本号
支持扫描网络目标数	当前产品内系统支持执行系统扫描目标的总数目
最大并发主机数	当前产品同一时间内系统支持执行的系统扫描任务中所有主机的最大数目
应用漏洞版本	当前产品应用漏洞版本号
支持扫描应用目标数	当前产品内系统支持执行应用扫描目标的总数目
最大并发域名数	当前产品同一时间内系统支持执行的应用扫描任务中所有域名的最大数目
基线核查策略版本	当前产品基线核查策略版本号
支持扫描基线目标数	当前产品内系统支持执行基线核查目标的总数目
公司	公司名称
官网	公司官网地址
使用到期时间	当前产品使用到期时间
维保到期时间	当前产品维保到期时间
合作单位	CNNVD 兼容认证
激活产品授权	点击查看序列号，复制序列号提供给厂家进行授权，然后复制激活码进行产品激活
允许扫描资产列表	查看允许扫描的资料列表