**开源软件供应链分析系统功能规范文档**

南京治煜信息科技有限公司

目录

[1. 引言 5](#_Toc8571)

[1.1 编写目的 5](#_Toc13920)

[2. 功能设计 5](#_Toc30787)

[2.1 功能概述 5](#_Toc10198)

[2.1.1 检测结果 5](#_Toc5269)

[2.1.2 检测统计 5](#_Toc2655)

[2.1.3 在用资产 6](#_Toc10657)

[2.1.4 资产管理 6](#_Toc27627)

[2.1.5 资产管控 6](#_Toc7947)

[2.1.6 私服管理 6](#_Toc18722)

[2.1.7 检测记录 7](#_Toc11305)

[2.1.8 组织及权限管理 7](#_Toc7204)

[2.1.9 检测配置 7](#_Toc2608)

[2.1.10 缺陷跟踪配置 7](#_Toc10880)

[2.1.11 通知配置 8](#_Toc23778)

[2.1.12 PDF报告设置 8](#_Toc21433)

[2.1.13 系统日志下载 8](#_Toc11632)

[2.1.14 License认证更新 8](#_Toc27914)

[2.1.15 基因库查询 9](#_Toc29104)

[2.1.16 漏洞预警 9](#_Toc23633)

[2.1.17 扫描通知 9](#_Toc10720)

[2.1.18 操作日志 9](#_Toc29512)

[2.1.19 API接口文档 10](#_Toc12675)

[2.1.20 访问令牌 10](#_Toc21868)

[2.1.21 IDE插件 10](#_Toc1049)

[2.1.22 CI/CD集成 10](#_Toc17990)

[2.1.23 私服防火墙插件 11](#_Toc31950)

[3使用说明 11](#_Toc27390)

[3.1登录 11](#_Toc4167)

[3.2项目检测 12](#_Toc8527)

[3.2.1发起检测 12](#_Toc14907)

[3.2.2检测结果 20](#_Toc24412)

[3.2.3检测统计 39](#_Toc25725)

[3.3在用资产 40](#_Toc27385)

[3.3.1组件 40](#_Toc31645)

[3.3.2漏洞 41](#_Toc27740)

[3.3.3许可证 42](#_Toc17740)

[3.4资产管理 44](#_Toc16226)

[3.4.1自研组件管理 44](#_Toc28453)

[3.4.2许可证管理 47](#_Toc16312)

[3.4.3漏洞管理 52](#_Toc16531)

[3.5资产管控 54](#_Toc28600)

[3.5.1黑白名单管理 54](#_Toc28890)

[3.5.2策略管理 57](#_Toc5812)

[3.6私服管理 61](#_Toc27288)

[3.6.1私服连接配置 61](#_Toc6911)

[3.6.2私服仓库管理 62](#_Toc20547)

[3.6.3仓库组件检测 64](#_Toc15617)

[3.6.4仓库组件查看 65](#_Toc29016)

[3.6.5防火墙策略配置 66](#_Toc17422)

[3.6.6防火墙阻断操作 67](#_Toc7782)

[3.7检测记录 68](#_Toc29408)

[3.8组织及权限管理 75](#_Toc31260)

[3.9 检测配置 81](#_Toc2267)

[3.10缺陷跟踪配置 84](#_Toc6135)

[3.11通知配置 89](#_Toc32395)

[3.11.1 邮件配置 89](#_Toc32077)

[3.11.2 钉钉配置 92](#_Toc24313)

[3.11.3 企业微信配置 96](#_Toc32713)

[3.11.4 LDAP配置 100](#_Toc27856)

[3.12 PDF报告设置 101](#_Toc5257)

[3.13系统日志下载 104](#_Toc31071)

[3.14 License认证更新 105](#_Toc32136)

[3.15基因库查询 106](#_Toc17663)

[3.15.1查找组件 106](#_Toc28406)

[3.15.2查找坐标 108](#_Toc15211)

[3.15.3查找漏洞 109](#_Toc21674)

[3.15.4查找许可证 110](#_Toc13318)

[3.16漏洞预警 111](#_Toc24535)

[3.17扫描通知 112](#_Toc23847)

[3.18操作日志 113](#_Toc1955)

[3.19 API接口文档 114](#_Toc29403)

[3.20访问令牌 115](#_Toc15197)

[3.21 IDE插件 117](#_Toc9418)

[3.22 CI/CD集成 118](#_Toc15192)

[3.23私服防火墙插件 118](#_Toc27674)

# 1. 引言

## 1.1 编写目的

本功能规范文档旨在详细描述智能泛在感知网前端设备脆弱性检测系统的功能设计和使用说明，供开发人员、测试人员和用户参考。通过本文档，用户可以全面了解系统的功能及其实现方式，从而更好地使用和维护系统，确保系统在实际应用中的有效性和可靠性。

# 2. 功能设计

## 2.1 功能概述

### 2.1.1 登录

登录功能需要用户填写信息进行登录操作，包括用户名，密码，验证码。用户可以通过该功能进入系统，从而采取相应的措施。

### 2.1.2 登出

用户可以通过登出功能注销当前用户的登录状态。

### 2.1.3 首页

用户登录成功后进入首页，首页显示内容包括：漏洞数据、高危资产TOP10、漏洞排行TOP10等，用户通过该功能可查看关键漏洞数据，快速、准确的了解漏洞信息。

### 2.1.4 管理员

管理员功能提供对用户的管理，包括新增用户、用户角色选择，启用、删除、编辑、重置密码等操作，默认已配置好角色权限，管理员仅需对用户进行角色选择即可。管理员可以通过该功能配置用户的角色和添加，确保系统的安全性和管理的有效性。

### 2.1.5 服务器状态

服务器状态功能提供对当前服务器设备运行状态的查看，包括系统信息、磁盘、CPU、内存的使用情况。用户可以通过该功能查看系统运行状态，确保系统运行的稳定性。

### 2.1.6 策略管理

策略管理功能提供对系统中所有扫描策略的管理，包括新建策略、修改、删除、查询、重置。其中新建和修改策略配置包括策略名称、策略配置（如并发数量、超时设置、探活轮次、速率限制等）、模板配置等。用户可以通过该功能查看和管理系统中的所有策略，可以通过该功能自定义策略配置。

### 2.1.7 扫描任务

扫描任务功能提供对系统中所有扫描任务的管理，包括新建任务、启动、停止、查看、导出、删除、查询、重置。其中新建任务配置包括扫描任务、执行方式、IP类型、扫描区域、扫描策略等。用户可以通过该功能查看和管理系统中的所有扫描任务信息，可以通过该功能自定义扫描配置，确保扫描结果的准确性和全面性。

扫描任务完成后，用户可以通过导出数据看到的本次扫描的详细信息列表，包括漏洞名称、对应主机、URL等。此外导出数据也包括对漏洞TOP10数量、比例等进行统计后的结果，用户可以通过该功能清晰明了的查看本次扫描的详细结果。

### 2.1.8 资产管理

资产管理功能提供对系统中所有资产的查看和区域的管理，包括新增区域、修改、删除、查询、重置。新增区域配置包括区域名称和IP泛微等。用户可以通过该功能查看和管理项目中的所有资产，确保资产的安全性和合规性。

### 2.1.9 漏洞管理

漏洞管理功能提供对系统中所有漏洞的详细信息，包括编号、名称、等级、描述、修复方式等。用户可以通过该功能了解到漏洞的描述及修复等。

# 3使用说明

## 3.1登录

确保服务是开启的，访问服务端：打开浏览器后，在地址栏中输入以下地址及端口号，登录地址参考：http://服务器IP地址，如下图所示。系统在默认安装好后提供用户名和密码。系统提交用户名和密码加验证码经过权限认证后可以进入系统系统管理员提供默认登录用户信息：用户名： admin，密码：向指定技术人员获取，被邀请的用户可根据接收到的邮件进行登录。

说明：推荐使用Google Chrome浏览器体验效果更佳

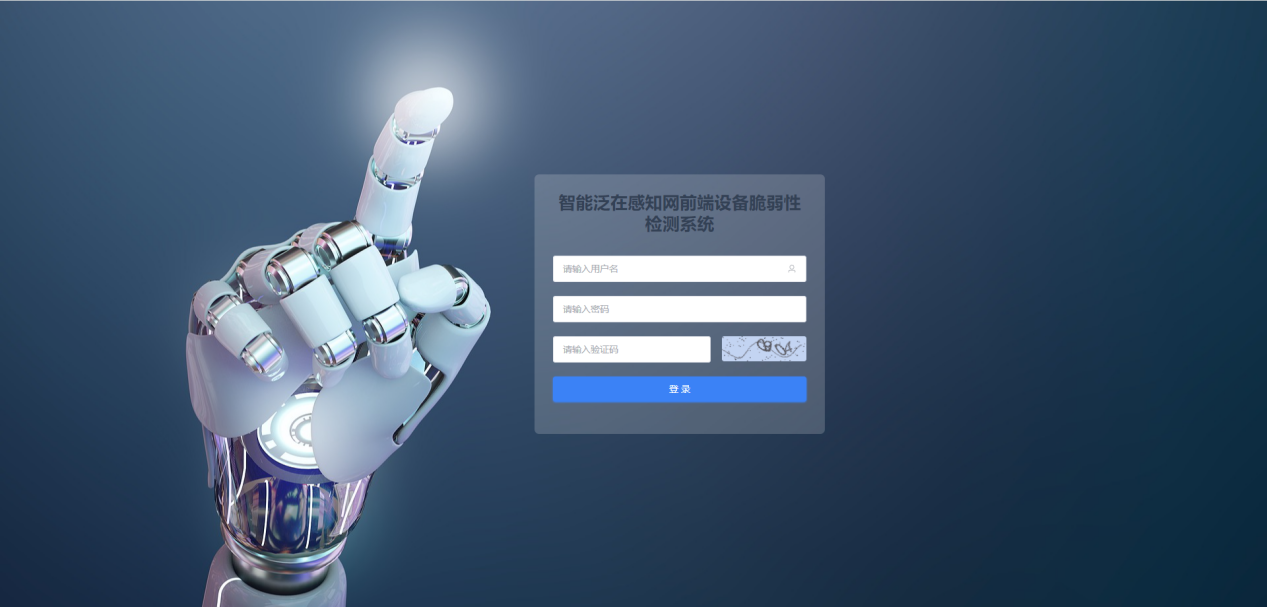


图 产品登录

## 3.2登出

系统通过登出注销用户的登录状态。



图 用户登出

## 3.3首页

* 漏洞数据：超危漏洞、高危漏洞、中危漏洞、低危漏洞
* 高危资产TOP10: 表格包括IP, 总漏洞数量，超危数量，高危数量，中危数量
* 漏洞排行TOP10: 表格包括漏洞类型，漏洞数量，漏洞等

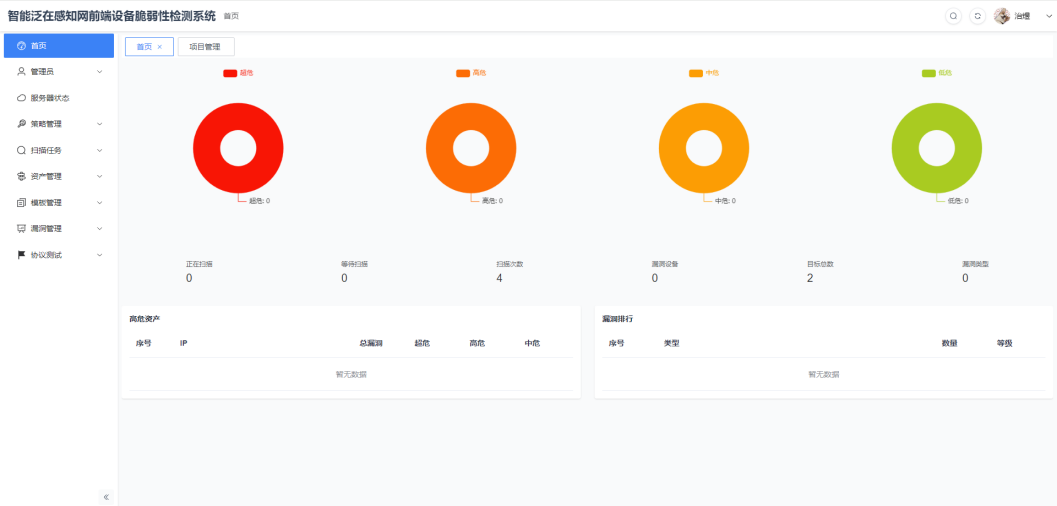


图 首页

## 3.4管理员

* 用户管理-新增用户：点击新增用户按钮会弹出表单内容包括：用户名、密码、昵称、用户角色必填项和手机号、邮箱、头像非必填，默认是启用状态

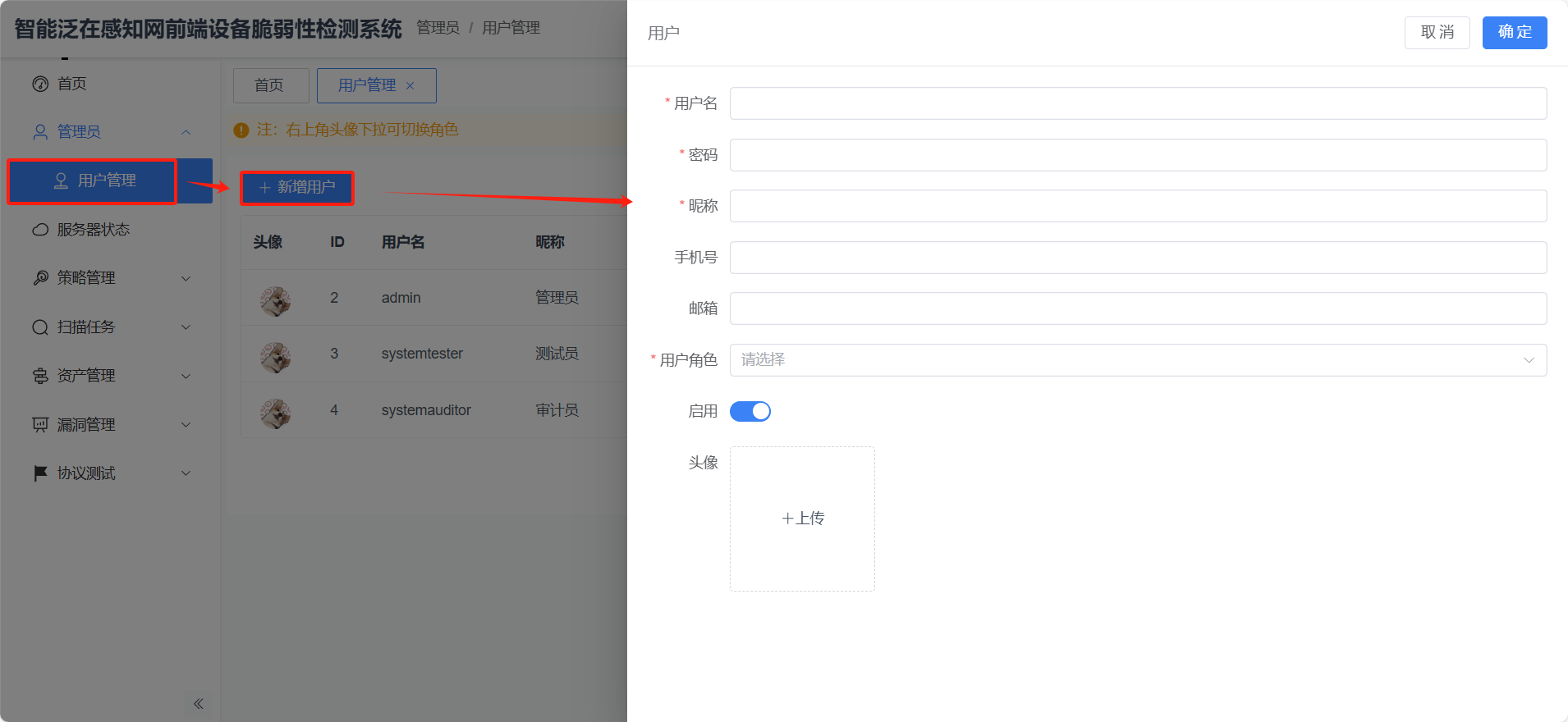


图 新增用户

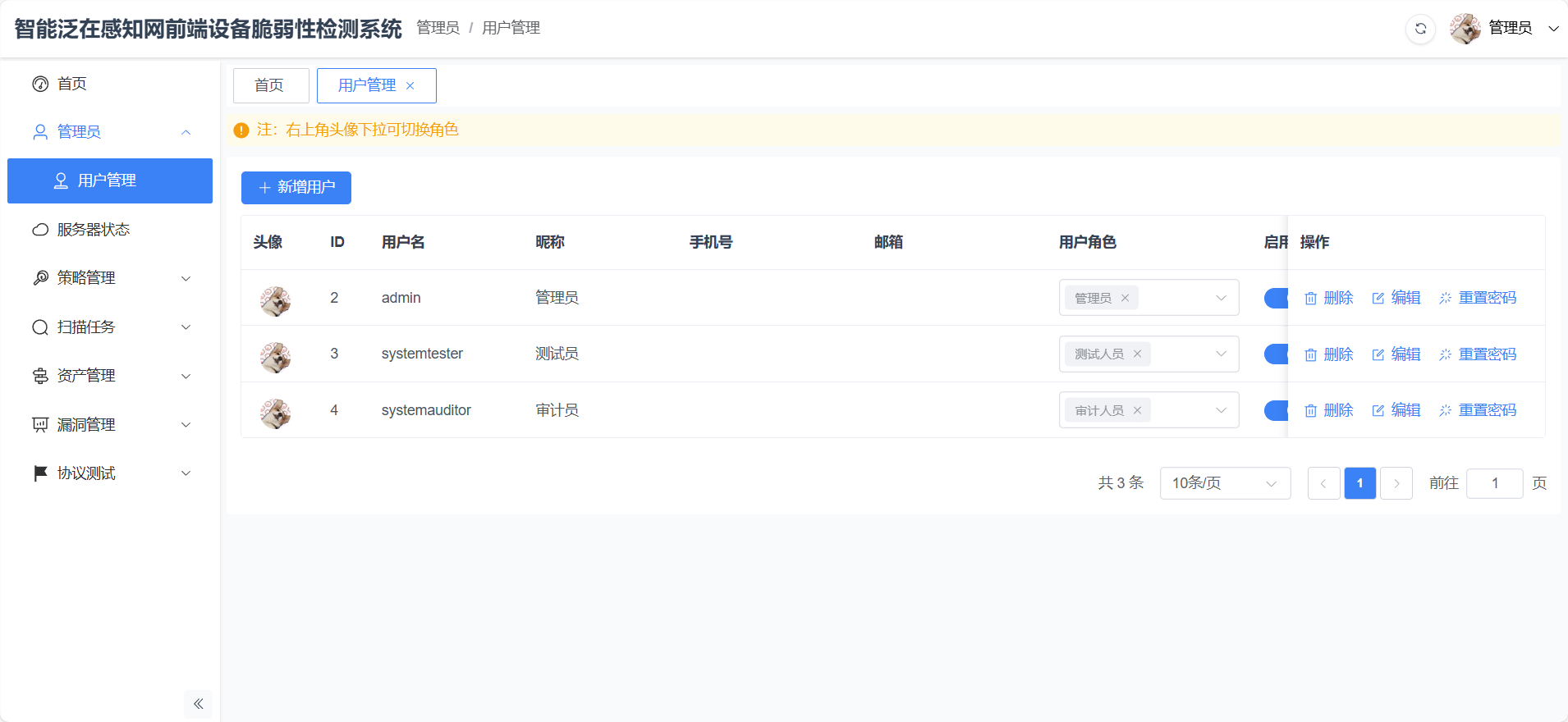


图 用户列表

* 用户管理-用户角色：用户列表的用户角色列可以自定义用户的角色(一个用户可以拥有多个角色)
* 用户管理-启用：默认创建用户是启用状态，可以在启用列选择对用户的账号启用和禁用，禁用后将不可以再登录
* 用户管理-删除用户：选择操作列中的删除，将删除对应行的数据，用户被删除后将无法使用账号
* 用户管理-编辑：选择列内的编辑可以修改用户昵称、手机号、邮箱、角色、启用状态、头像
* 用户管理-重置密码：重置密码将会把用户的密码重置为新增时的密码

## 3.5服务器状态

* 系统信息：系统运行环境和Go语音版本
* 磁盘信息：磁盘的容量大小和使用情况
* CPU信息：CPU的使用情况
* 内存信息：系统内存的使用情况

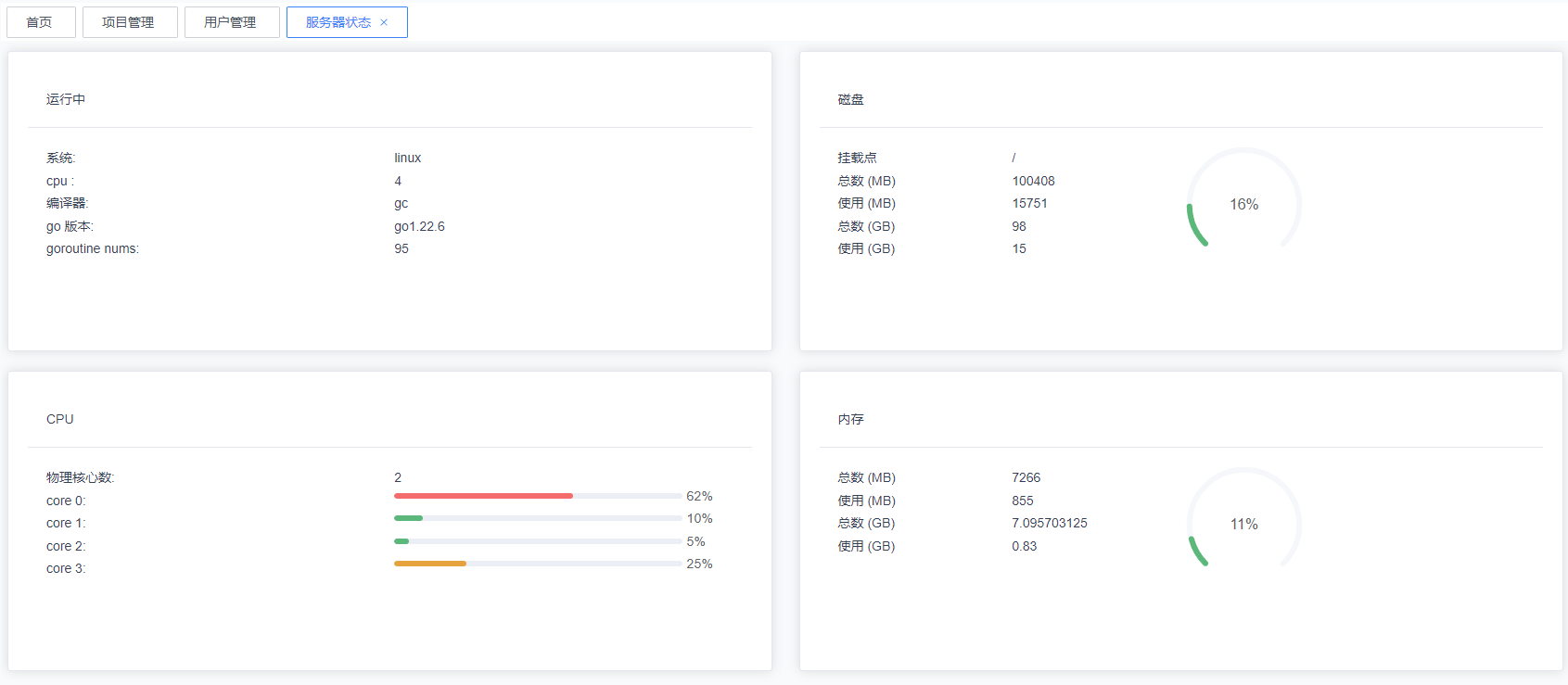


图 服务器状态

## 3.6策略管理

### 3.6.1创建策略

点击新增策略弹出表单内容包括：策略名称，

* 在线监测：默认开启在线监测，将勾选状态改为未选择，则改为不开启在线监测，并发数量默认3000，超时时间2秒，探活轮次1次，速度限制2000
* 端口检测：同在线监测相近，默认开启，端口范围分为 http，top100，top1000，80,90;并发数默认3000，超时2秒，探活轮次1次，速率限制2000
* 模板配置

模板分为三种类别：资产发现，漏洞扫描，弱口令，默认最大并发数是3000，超时设置2秒，限流速度2000，探活轮次1次，模板为全部模板，根据需求自定义需要扫描的类型模板，选择自定义时，可以根据设备类型，系统类型，厂商名称，产品型号，模板名称来搜索需要的模板，并勾选选中，然后保存。

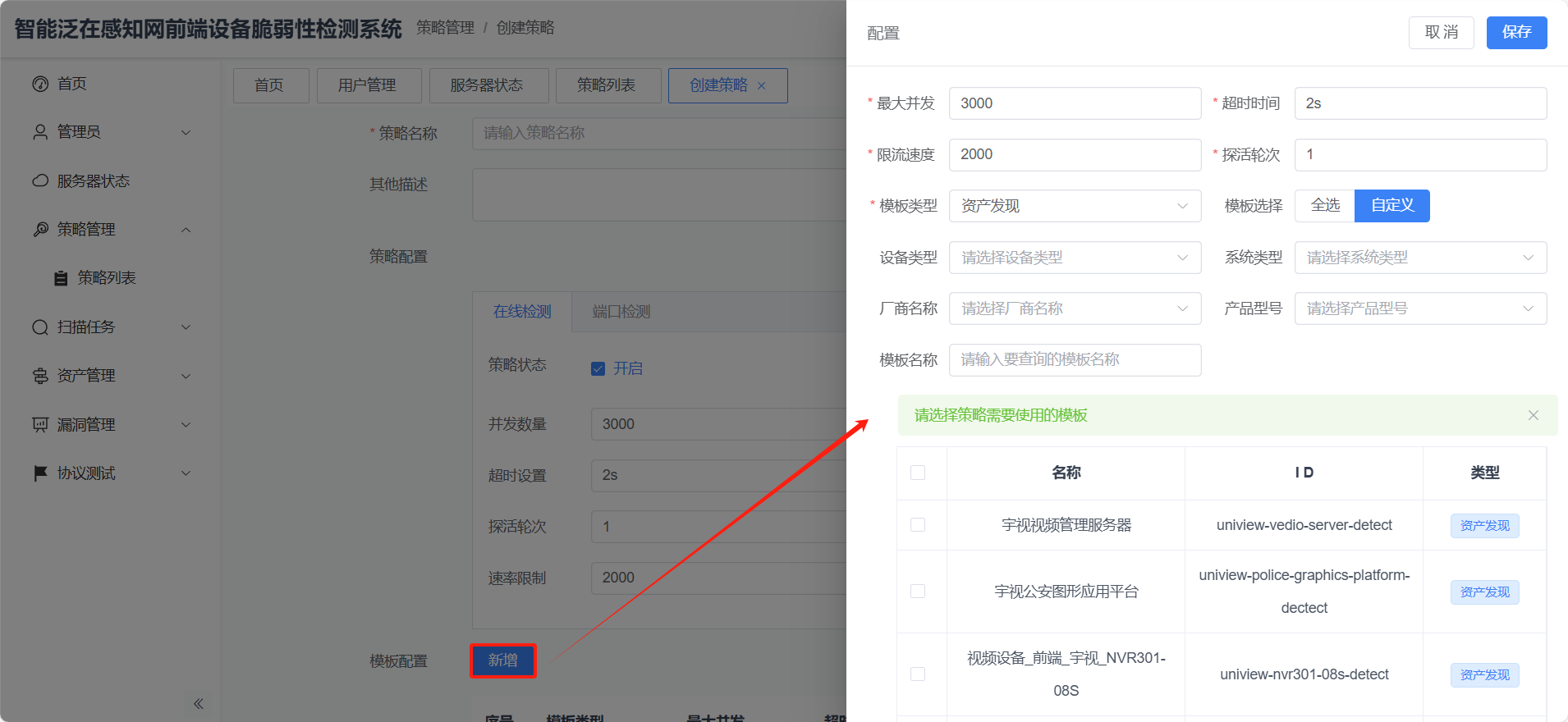


图 新建策略

### 3.6.2策略列表

展示目前所有策略，可以通过搜索条件：策略名称和扫描类型来筛选列表。对已有策略可进行修改和删除操作。修改策略方式和新增策略方式相同，内容可参考新增策略。底部带有分页系统，可以通过更改显示数据大小和跳转到指定页。

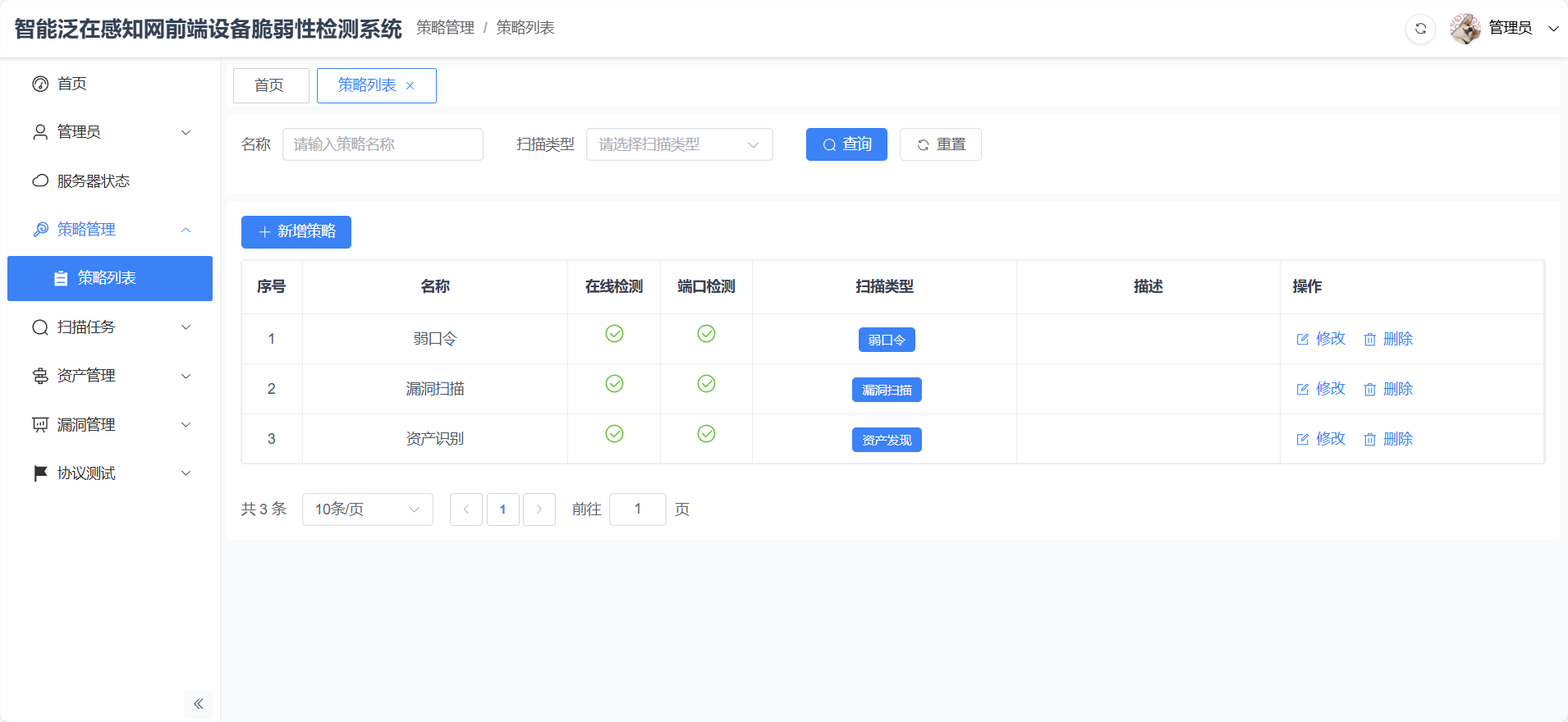
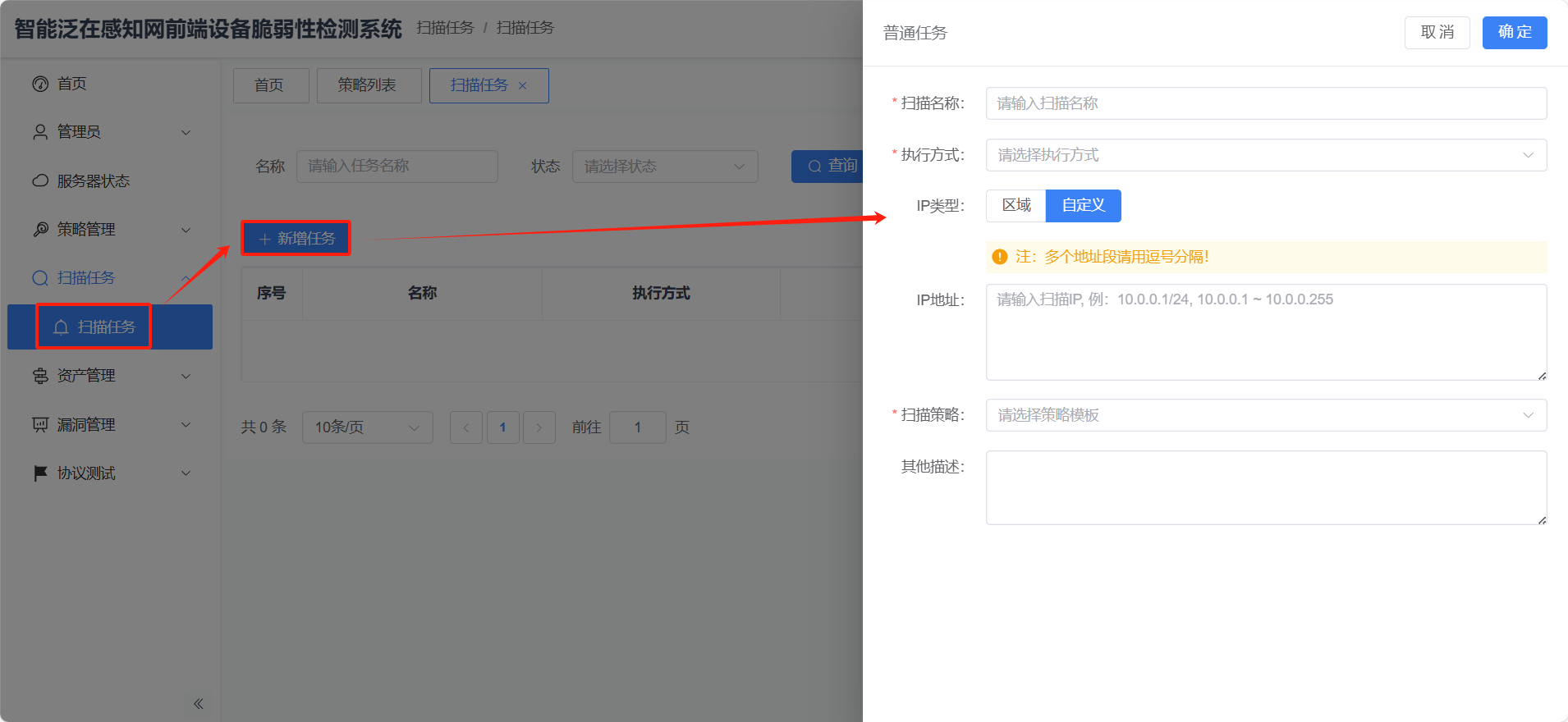


图 策略列表

## 3.7扫描任务

### 3.7.1新增普通任务

新增任务内容包括任务名称、执行方式(立即执行、稍后执行)、IP类型默认选择是扫描区域，需要自定义IP地址可以选择自定义，输入IP地址，格式为：10.0.0.1/24 或者是10.0.0.1 ~10.0.0.255，多个IP范围用英文逗号分隔；选择要关联扫描策略、输入任务描述，点击确定后提交。

图 新增任务

### 3.7.2任务列表

任务列表内容包括：任务名称、任务执行方式、引用策略、状态、启动操作、停止操作、查看任务内容操作、删除任务。

启动按钮：当任务执行方式是稍后执行、已完成、失败可以点击启动按钮再次执行。

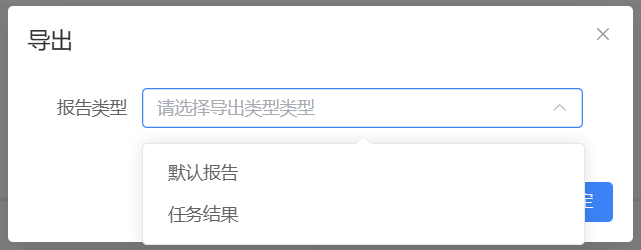
查看按钮：点击查看按钮可以查看当前任务执行的信息包括：扫描IP,关联策略，执行方式，任务名称，当前状态，执行步骤，执行进度。

停止按钮：在显示停止按钮的行点击停止会立即停止正在执行的任务。删除按钮：点击删除，回弹出提示是否删除，如果确认删除任务，将会从列表删除这个任务内容。

图 任务列表

### 3.7.3导出报告

执行完成的任务点击导出按钮可以选择导出报告的格式及内容。报告分为两种格式：默认报告和任务结果，默认报告为结果统计，任务结果为数据列表。



## 3.8资产管理

### 3.8.1资产列表

此页面展示扫描任务执行后的资产，包括名称、IP、设备类型、开放端口，可以根据搜索条件进行检索。



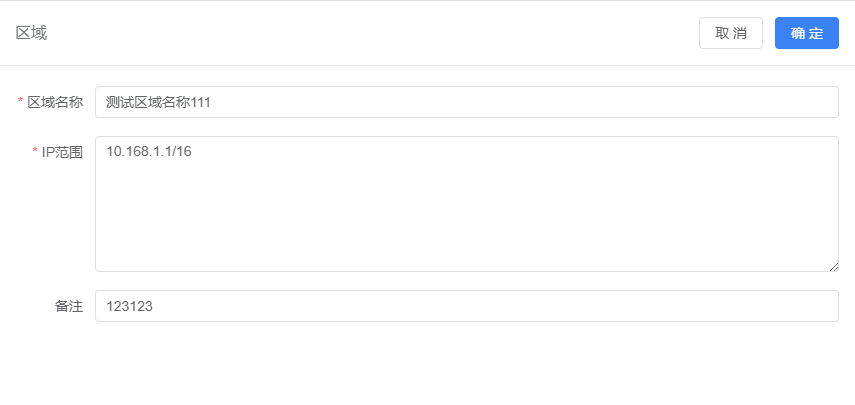
### 3.8.2区域列表

此页面展示目前区域的设定包括，区域名称、区域内的IP地址池、备注。可进行修改、删除操作。修改区域参考新增区域内容。点击列表内操作下的删除按钮会将当前选择区域删除。



### 3.8.3新增区域

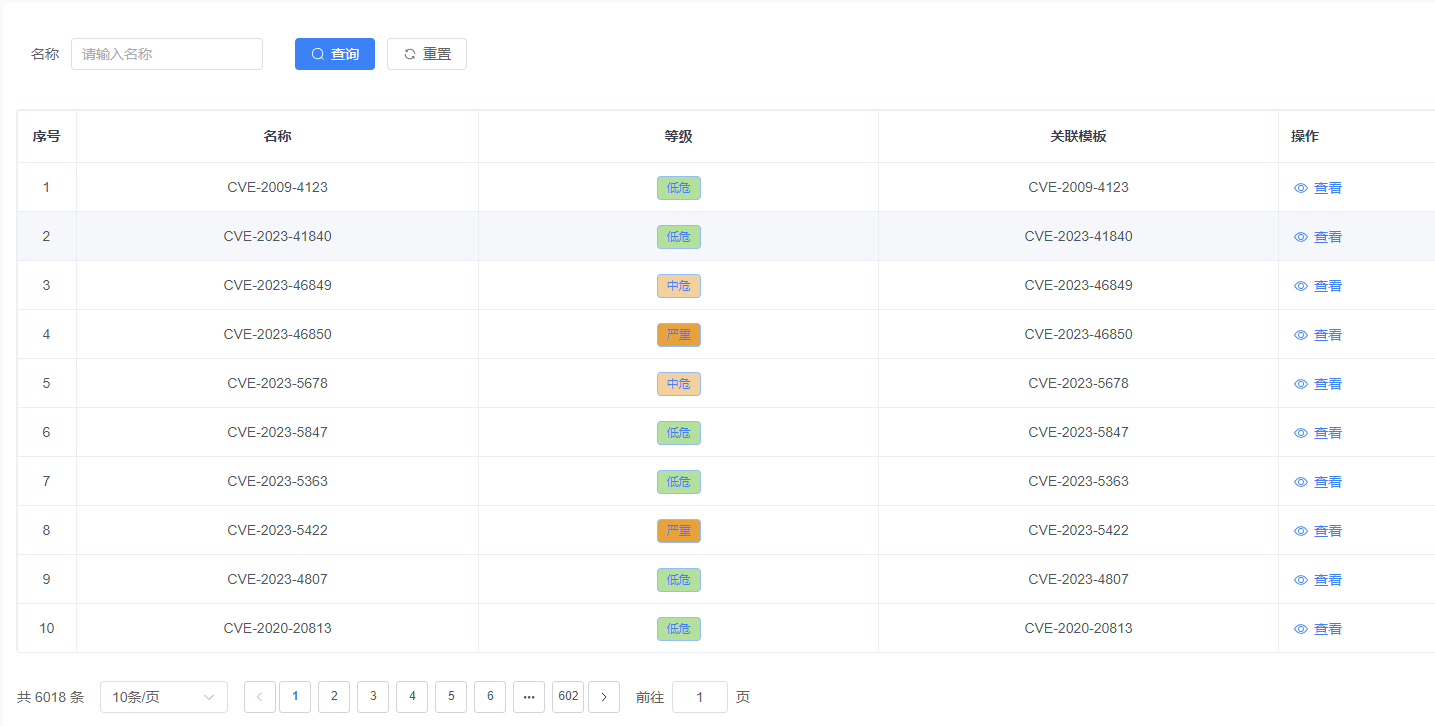
必填项区域名称、IP范围（支持类型：10.0.0.1/16，10.0.0.1~10.255.255.255，多个IP范围用英文逗号分隔），备注选填。



## 3.9漏洞管理

### 3.9.1漏洞数据库列表

此页面展示数据库中漏洞信息，包括名称、等级、关联模板，可以根据搜索条件进行检索。



### 3.9.2查看按钮

点击查看，会弹出当前漏洞对应的介绍信息。

