AiLPHA 资产弱点管理平台

—用户使用手册

杭州安恒信息技术股份有限公司

目 录

1. 产品简介

1.1. 产品特性

1.1.1. 资产管理能力

- 支持 EXCEL 导入；
- 支持从 CMDB 或 ITSM 系统同步资产；
- 支持人工录入资产信息；
- 支持通过扫描引擎发现资产；
- 支持通过资产检测探针发现；
- 支持 Android、web、IOS、公众号、小程序、H5 等应用资产；
- 支持主流的网络类、安全类设备、交换设备、路由设备、操作系统、应用系统和网络打印机等主机资产；
- 支持资产的基本信息管理，包括标签、资产重要性、资产责任人、资产所属业务系统和所属部门等信息；
- 对于主机类资产，支持操作系统及版本，设备类型，厂商及型号，开放端口、服务、协议，关联域名信息及 banner 等属性信息发现及管理；
- 对于网站类资产，支持开发语言及框架、web 服务器类型、web 组件、ICP 备案、子域名、关联 IP 等属性信息发现及管理。

1.1.2. 漏洞管理能力

- 支持通过扫描引擎扫描发现漏洞自动化收集；
- 支持通过安全服务人工渗透漏洞自动化收集；
- 支持第三方扫描引擎扫描结果数据导入，安恒远程评估、绿盟、Nessus 等；
- 支持收集的数据类型包括主机扫描、web 扫描、基线扫描、弱口令扫描、数据库扫描等结果数据；
- 支持内部运维人员运维发现漏洞通过人工录入或导入方式收集；
- 支持互联网公布漏洞通过人工录入或导入方式收集；
- 内置来自 CVE、CNNVD 等权威机构发布的完整漏洞，并定期更新出现的安全漏洞；
- ★支持集成多个扫描引擎的漏洞库；
- 支持将漏洞信息标记为误报，支持误报漏洞的查看、查询、单个取消误报及批量取消误报操作；
- 支持将漏洞信息标记为搁置，支持对搁置的漏洞的查看、查询、单个取消搁置及批量取消搁置操作。

1.1.3. 任务管理能力

- 支持通过 EXCEL、XML、HTML、CSV 导入第三方扫描引擎扫描报告方式创建漏洞扫描任务，第三

方扫描报告支持如下：安恒远程评估、绿盟、nessus、青藤云、sumap 等；

- 支持创建扫描任务，支持绿盟、安恒、nessus、青藤云、、sumap、铱讯等扫描工具；
- 支持选择主机扫描、WEB 扫描、基线扫描、数据库扫描以及弱口令扫描等扫描类型；
- 支持扫描任务的定时单次执行、立即执行；
- 支持漏洞扫描任务按每天、每周、每月、每年的任务计划进行周期调度，自动扫描，当新的高危漏洞发布时，更快速地评估安全风险。

1.1.4. 工单管理能力

- 支持漏洞进行工单的下发、整改、验证、关闭等全生命周期管理及工单流转状态显示；
- 支持工单的自动复扫和自动复扫的规则自定义；可配置漏洞复扫验证规则，规则要求灵活可配；
- ★支持工单自动下发的规则自定义，支持 SOAR 方式自动化编排，在漏洞下发时，提供自动化匹配规则功能，漏洞匹配规则动态可配，以便应对漏洞整改业务的动态变化，同时规则配置需支持将主机的业务、系统分离派单，以满足动态的漏洞修复工作变动；
- ★支持漏洞下发时，遵循最小工作量原则，漏洞自动去重下发；
- ★支持自定义工单流转流程，定义各流转节点的人员群组、功能；

1.1.5. 统计分析能力

- 支持支持从资产、扫描任务、漏洞、扫描引擎等多个维度进行智能的综合性分析；
- 支持从资产风险分布、业务系统分布、责任人资产分布、资产类型分布等维度统计分析；
- 支持从资产、业务系统、责任人等视角、资产类型、漏洞级别等维度进行查询并展示资产与漏洞相关信息；
- 支持从资产趋势视角、资产风险视角、漏洞视角等维度展示扫描相关信息；
- 支持从漏洞风险分布、服务分布 TOP10、端口分布 TOP10 等维度统计分析；
- 支持从漏洞名称、服务类型、CVE 编号、漏洞等级等条件查询并展示漏洞信息；
- 基于同资产的两次不同扫描引擎扫描结果比对不同扫描引擎间针对不同主机扫描能力、弱口令扫描能力、基线扫描能力等其他维度的扫描能力进行比对。

1.1.6. 告警通知能力

- 支持分析报告、扫描引擎调度进度、工单流转状态等信息进行邮件通知；
- 支持通过邮件方式来发送指定内容；
- 支持通过短信方式来发送指定内容；
- 支持与大数据平台及其他平台对接；
- 主要将资产端口信息和漏洞信息等内容推送到大数据平台。

1.1.7. 其他亮点能力

- 支持对与资产相关、扫描任务相关、工单相关等配置进行默认设置。

1.2. 产品概述

AiLPHA 资产弱点管理平台，作为 IT 系统漏洞进行自动化的检测管理工具，通过对客户各类扫描工具的统一调用，收集管理来计算环境中各种资产的信息，快速高效完成漏洞扫描，并对结果数据进行存储、分析、挖掘和处置服务，提升全网自动化漏洞检测管理的能力，规范全网安全漏洞管理的标准，及时发现各种安全威胁，为管理人员提供全局的视角，确保客户业务的不间断运营安全；AiLPHA 资产弱点管理平台通过在本平台创建扫描任务并审核通过后可以自动下发任务到各扫描引擎，扫描完成后自动对结果进行分析，帮助用户从资产、漏洞多维度分析资产组在多次扫描后，资产的风险值趋势、漏洞修复情况等信息，并提供反馈信息给对方修复使用，实现信息资产的统一管理、监控资产的健康状况，协助用户全面审计信息系统整体安全状况。

2. WEB 概述

2.1. 功能简介

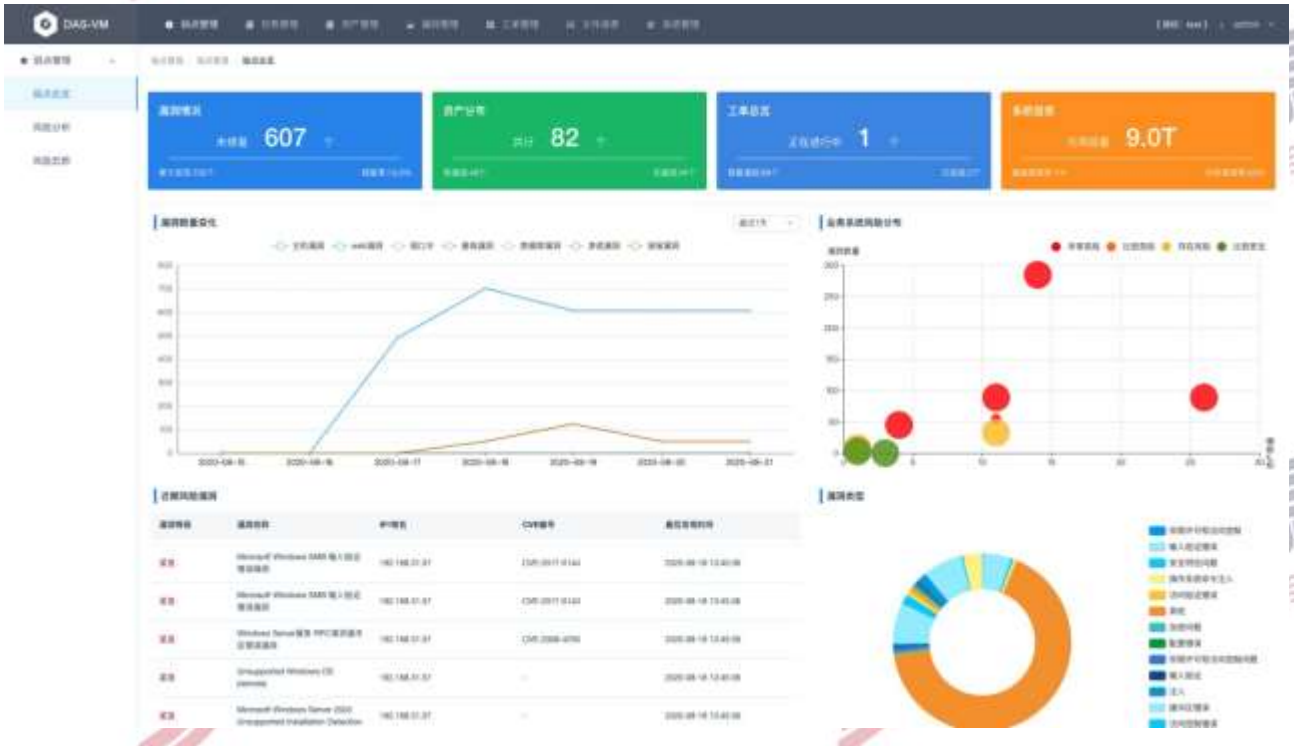
通过 WEB 方式管理漏洞管理平台。

2.2. WEB 登录

2.2.1. 通用版本

（1）在浏览器中输入 *https://*管理 *IP*，进入登录窗口。

（2）在登录窗口中输入用户名、密码、验证码，点击<登录>按钮后，跳转至扫描主页。



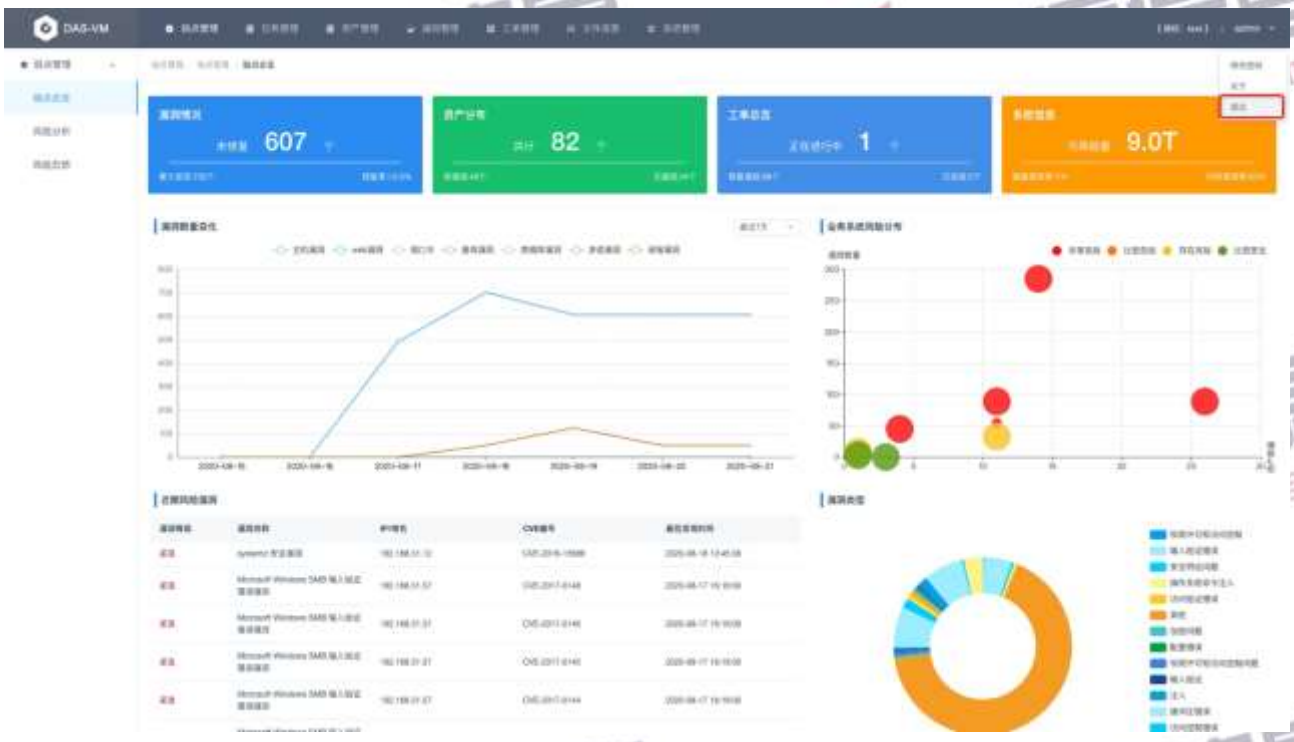
说明

浏览器目前支持 Chrome、火狐浏览器 。

出厂默认用户名/密码为：admin/r0x@z9lHw1c。

2.3. 退出 WEB 登录

（1） 在漏洞管理平台管理页面上右上角单击用户名，然后点击下拉的<退出>按钮，退出 WEB 登录。退出系统时，系统不会自动保存当前配置。因此建议用户在退出系统前先设置保存当前配置。



注意

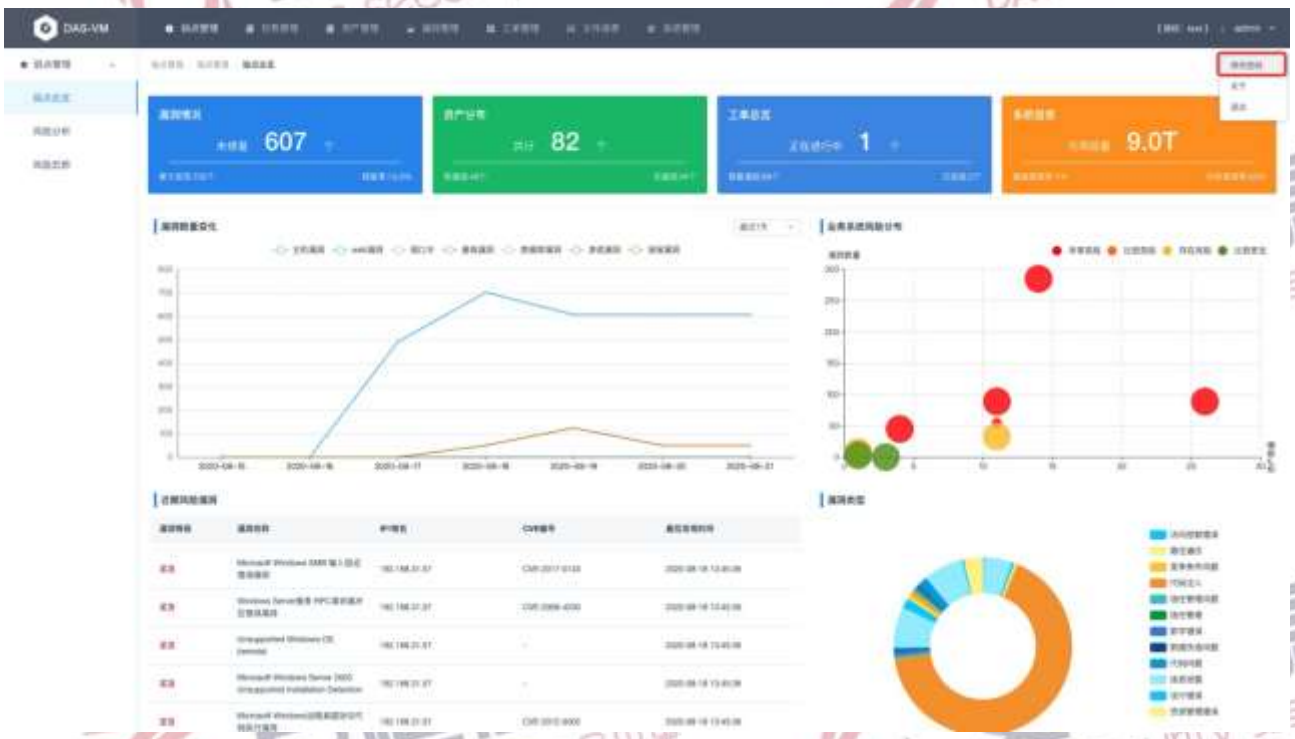
通过直接关闭浏览器标签的方式，已登录到设备上的用户不能自动退出登录。

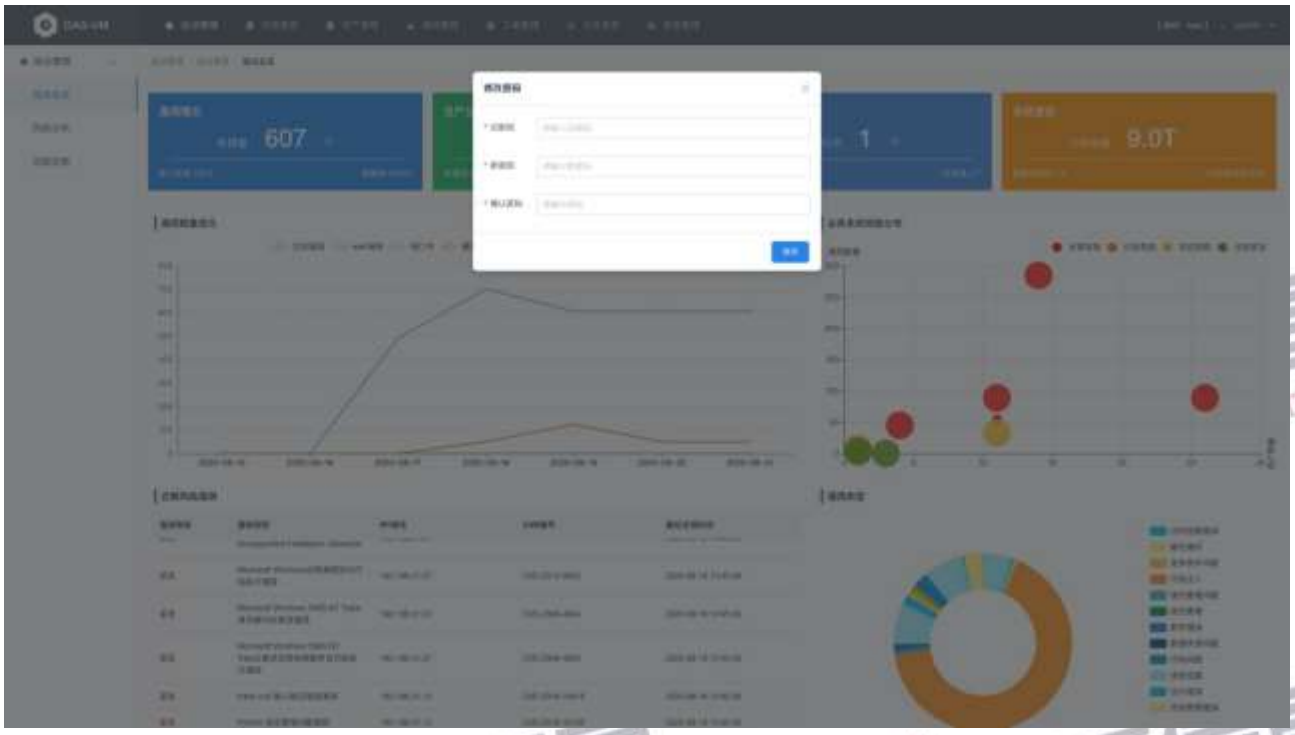
2.4. 关于版本

（1） 在漏洞管理平台管理页面上右上角单击用户名，然后点击下拉的<关于>按钮，弹出关于漏洞平台的版本信息窗。

2.5. 修改密码

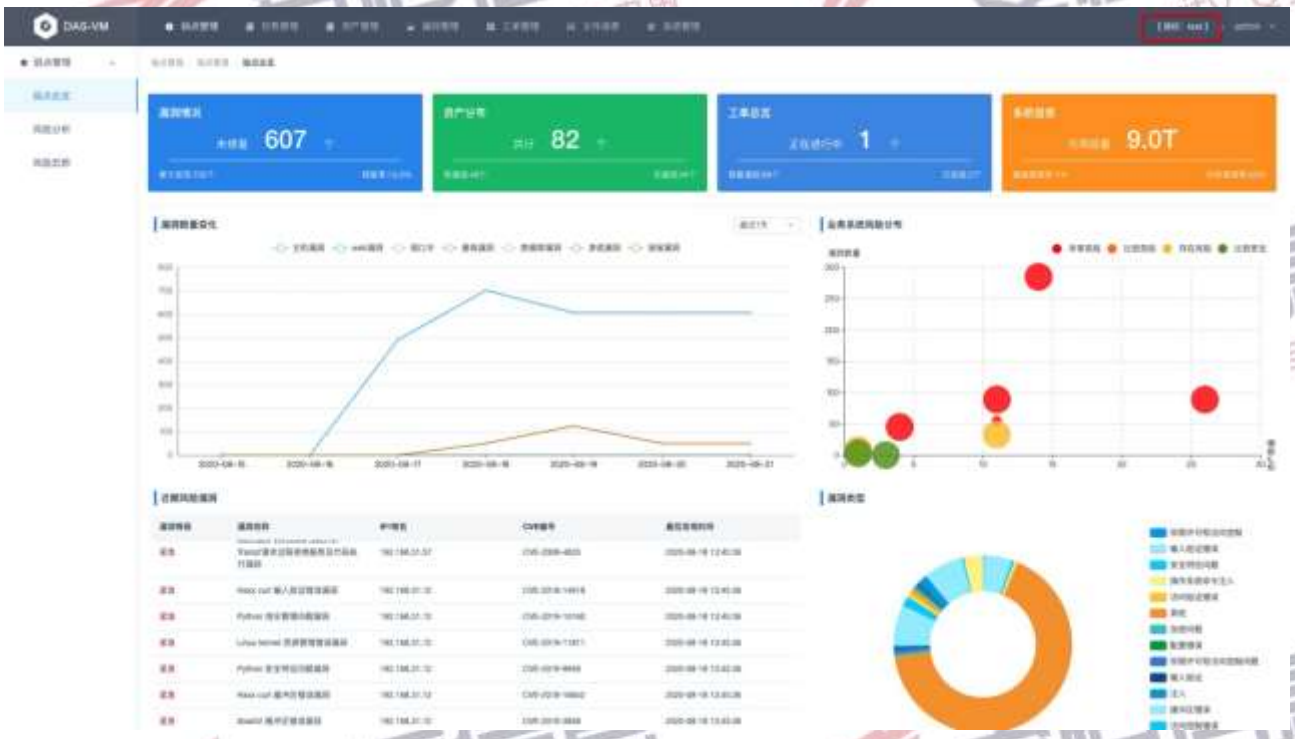
（1） 在漏洞管理平台管理页面上右上角单击用户名，然后点击下拉的<修改密码>按钮，修改漏洞平台用户的密码。





2.6. 许可授权

（1） 在漏洞管理平台管理页面上右上角单击授权名称，页面跳转至许可证书页。



2.7. WEB 页面布局

WEB 页面布局共分为：功能页签、管理链接、导航树和操作区四部分。

WEB 页面布局说明见下表：

序号	名称	说明
(1)	功能页签	以不同的角度提供了各类管理功能的配置入口，方便管理员根据实际需要进行切换
(2)	管理链接	查看当前授权信息、登录用户信息、系统信息、修改密码以及退出等相关功能链接
(3)	导航树	列出了当前功能页签对应的操作链接
(4)	操作区	该区域主要用于信息展示以及相关功能的操作

3. 弱点管理

3.1. 弱点管理

3.1.1. 弱点总览

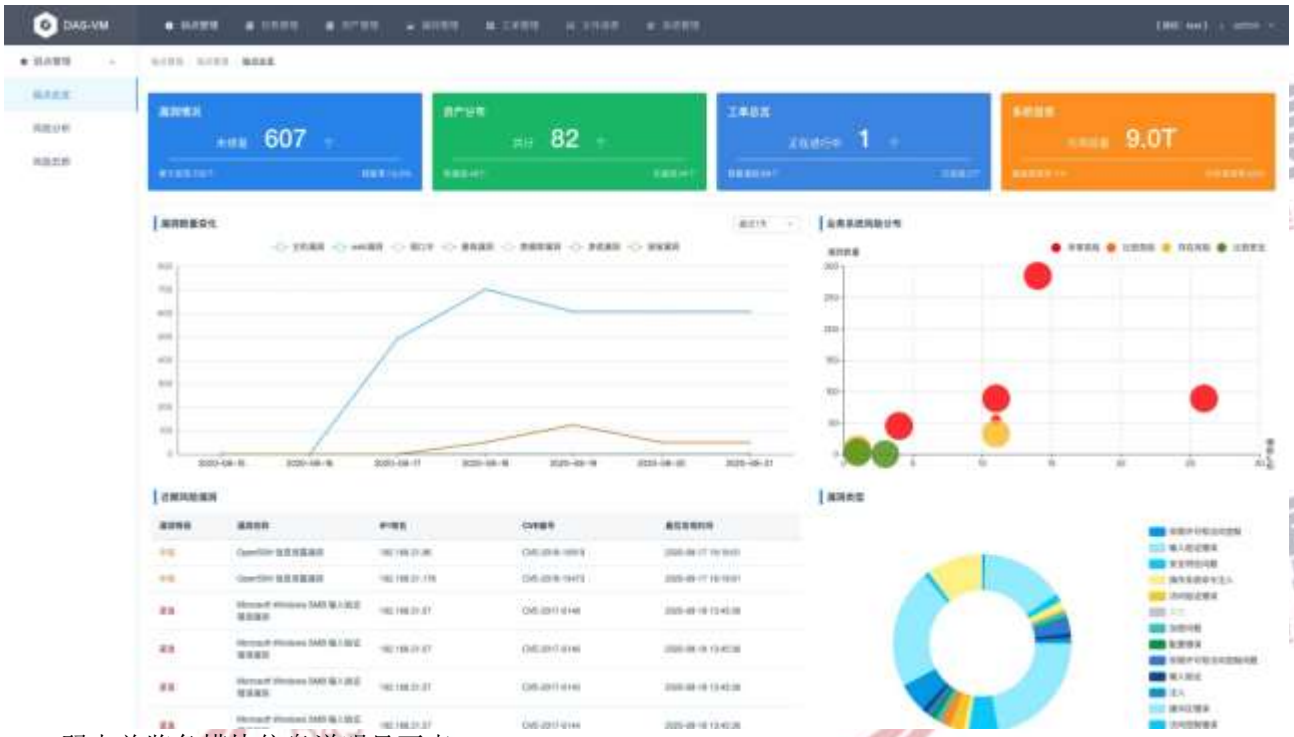
弱点总览可以帮助用户了解被扫描资产的扫描情况和状态，具体包括以下几个方面的内容：

- 漏洞情况，包括：当前未修复的漏洞，累计发现的有效漏洞数量，漏洞的修复率
- 资产分布，包括：资产总数、有漏洞资产数量、无漏洞资产数量
- 工单总览，包括：正在进行中的工单数量、累计通过工单修复的漏洞数量、已完成的工单数量
- 系统信息，包括：当前系统主程序所使用的目录可用空间，程序空间的使用率，当前内存的使用率
- 漏洞数量变化，包括：主机漏洞、web 漏洞、基线问题、数据库漏洞、弱口令、渗透测试漏洞、误报漏洞
- 业务系统分布散点图：展示各业务系统的风险程度

- 近期风险漏洞：动态显示最近 7 天内最新的 200 条风险漏洞（紧急、高危、中危 ）
- 漏洞类型：展示平台中未修复的漏洞种类分布

3.1.1.1. 弱点总览

（1）用户 WEB 登录后，进入[弱点管理 /弱点管理 /弱点总览]页面。



弱点总览各模块信息说明见下表：

模块	说明
漏洞情况	当前未修复的漏洞，累计发现的有效漏洞数量，漏洞的修复率
资产分布	资产总数、有漏洞资产数量、无漏洞资产数量
工单总览	正在进行中的工单数量、累计通过工单修复的漏洞数量、已完成的工单数量
系统信息	当前系统主程序所使用的目录可用空间，程序空间的使用率，当前内存的使用率。可以进行存储空间告警，当系统存储已用容量达到 95%时，首页系统信息展示警告图标，点击可弹出提示，正常存储情况不展示告警图标。
漏洞数量变化	包括：主机漏洞、web 漏洞、基线问题、数据库漏洞、弱口令、渗透测试漏洞、误报漏洞
时间范围	单击图标 最近7天 时间选择器，可以选择不同时间的时间段平台的扫描总览信息，如：最近 7 天、最近 30 天、最近一年、本月、本周
业务风险系统分布	横轴为业务系统资产数量，纵轴为业务系统漏洞数量，颜色代表业务系统安全程度，分为四阶，分别为非常危险、比较危险、比较安全、非常安全，散点半径与修复率成反比，修复率越高半径越小

近期风险漏洞	显示最近 7 天内最新的 200 条风险漏洞：紧急、高危、中危 ，累计筛选 200 条，按最新发现时间排序，同一发现时间按漏洞等级排序，动态展示
漏洞类型	展示平台中未修复的漏洞种类的分布

3.1.2. 风险分析

风险分析功能用于分析已经完成的扫描任务结果分析，分别从资产维度、任务维度、漏洞维度、扫描引擎对比四个维度进行分析。

3.1.2.1. 资产维度

资产维度 tab 页主要显示当前所有资产的资产风险值。

风险值：表示一个资产的安全风险，由资产上存在的漏洞等级、漏洞数量、资产重要性计算得出：

- **单个漏洞分值：**

  紧急 5 分　高危　4 分　中危 3 分　低危 1 分　信息 0.2 分（低危漏洞+信息漏洞分值最高影响 25 分）

- **基础分值：**

  当存在中危漏洞时风险值基础分+25，存在高危漏洞时风险值基础分+50，存在紧急漏洞时风险值基础分+75

- **计算方式：**

  资产风险值=sum（单个漏洞分值*资产重要性）+基础风险分值

  如一个资产存在 1 个紧急漏洞和 30 个低危漏洞，当资产重要性为 1 时，分值应为：

$$(5\times1+1\times30)\times1+75\Rightarrow5\times1+25+75=105\Rightarrow100$$

- **资产风险程度评级：**

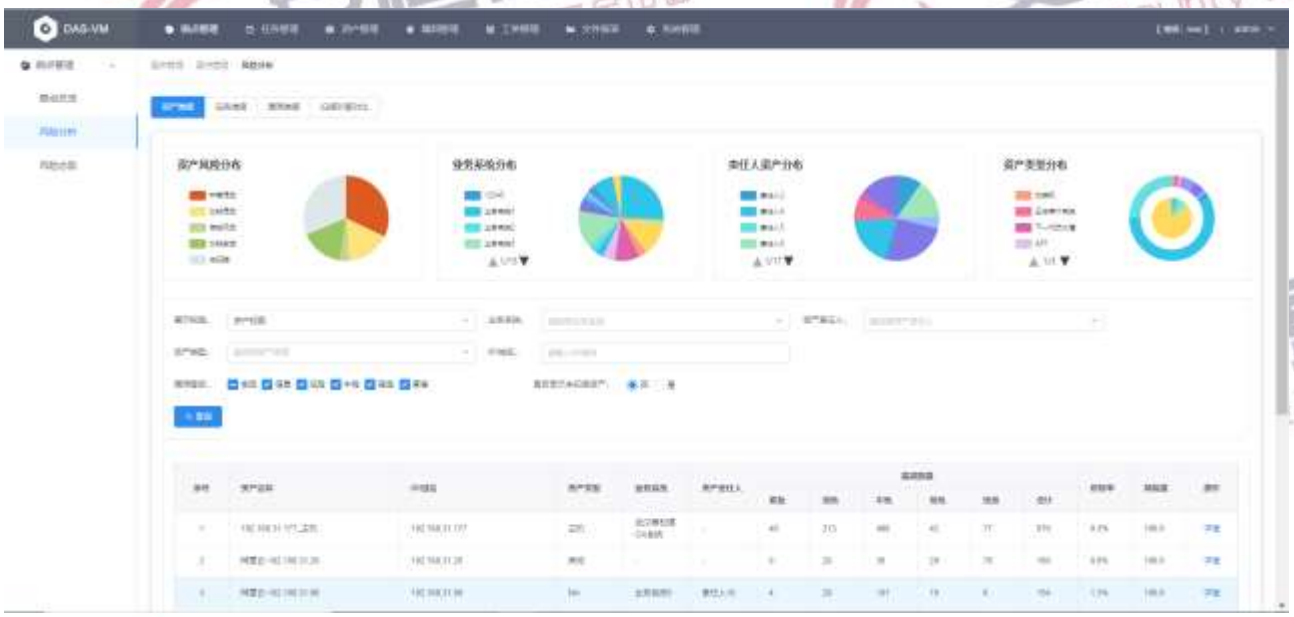
  非常危险：75<=资产风险值<=100

  比较危险：50<=资产风险值<75

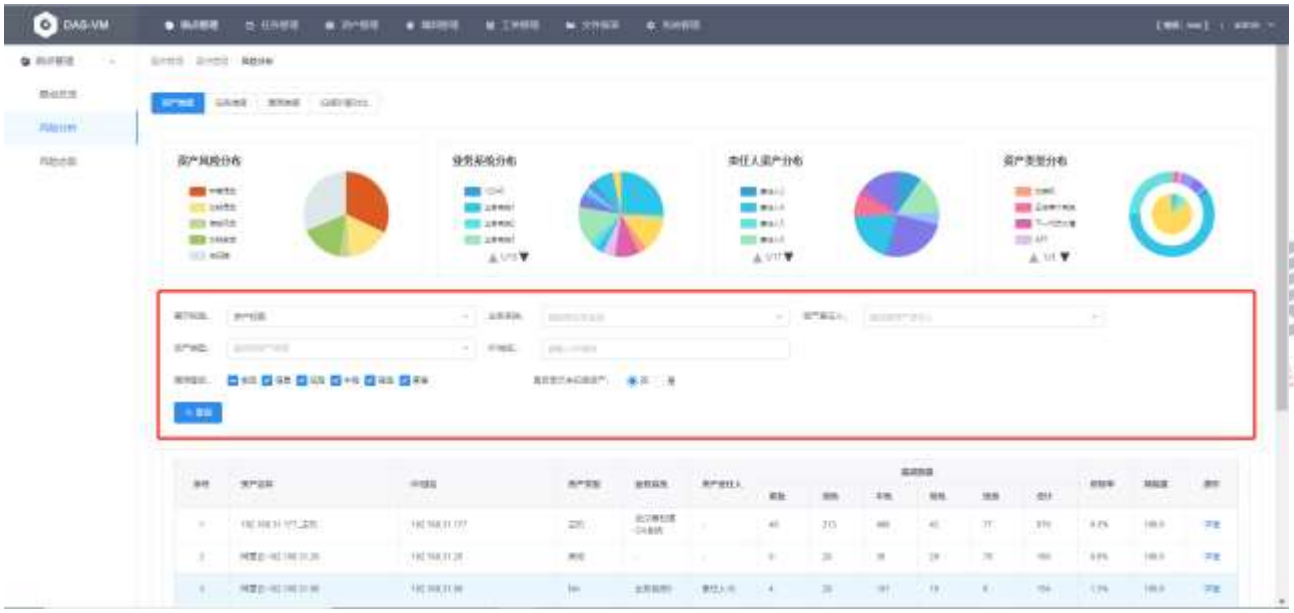
  存在风险：25<=资产风险值<50

  比较安全：0<=资产风险值<25

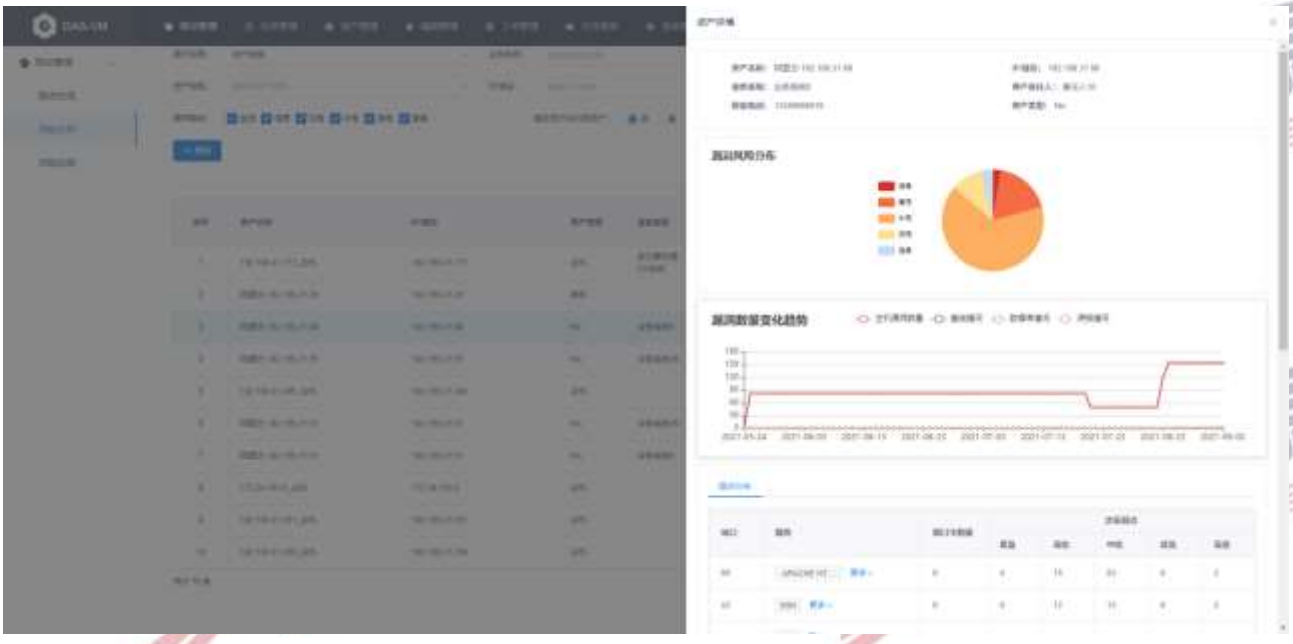
（1）用户 WEB 登录后，进入[弱点管理 /弱点管理 /风险分析]页面的资产维度 tab 页。



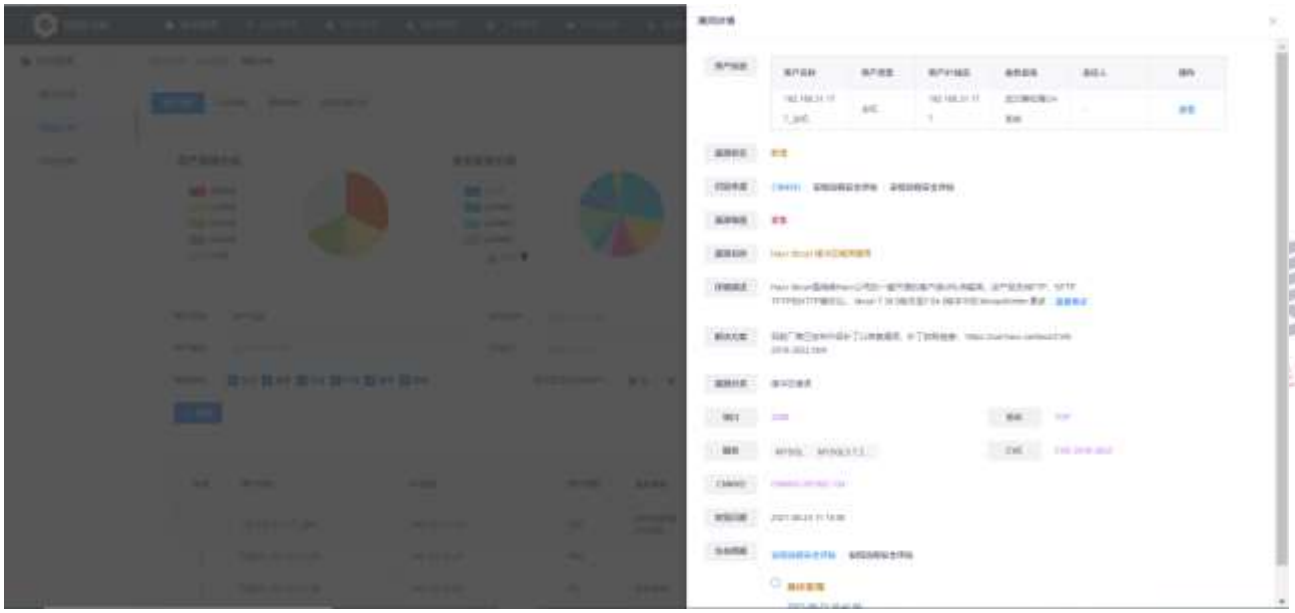
（2） 设置查询条件，点击<查询>按钮进行查询。



（3） 点击查询结果资产列表中操作列的<详情>按钮，可以查看该资产的资产详情。



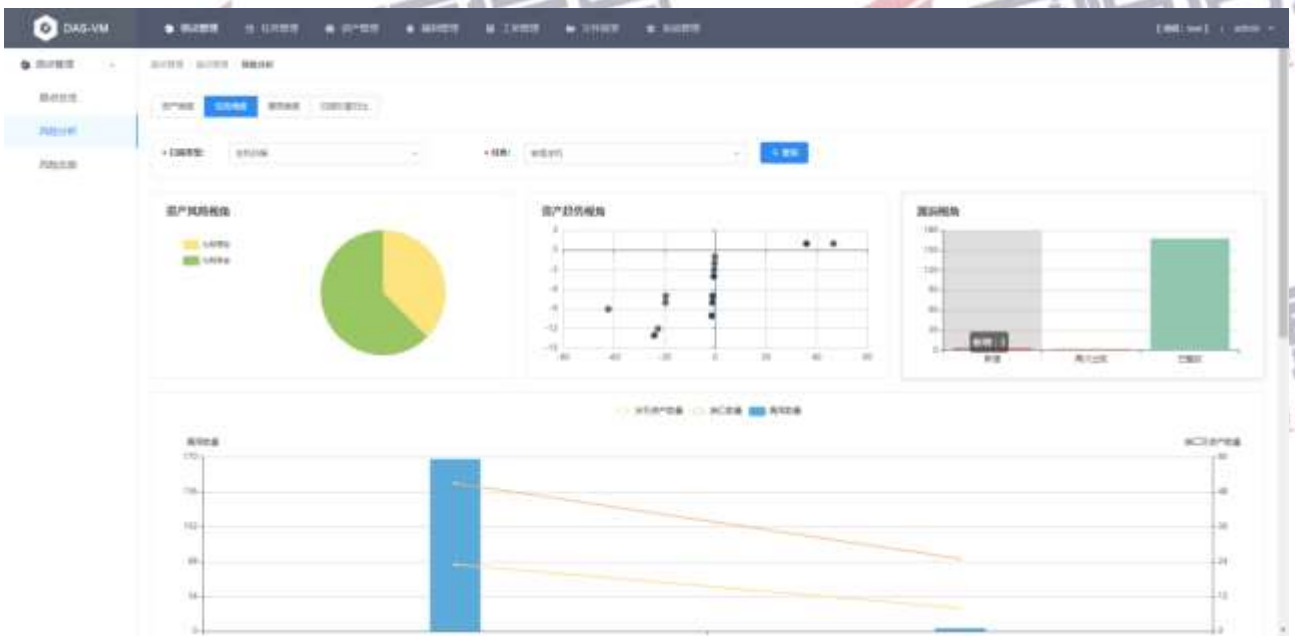
（4） 点击资产详情漏洞列表中漏洞的<详情>按钮，可以查看该漏洞的漏洞详情。



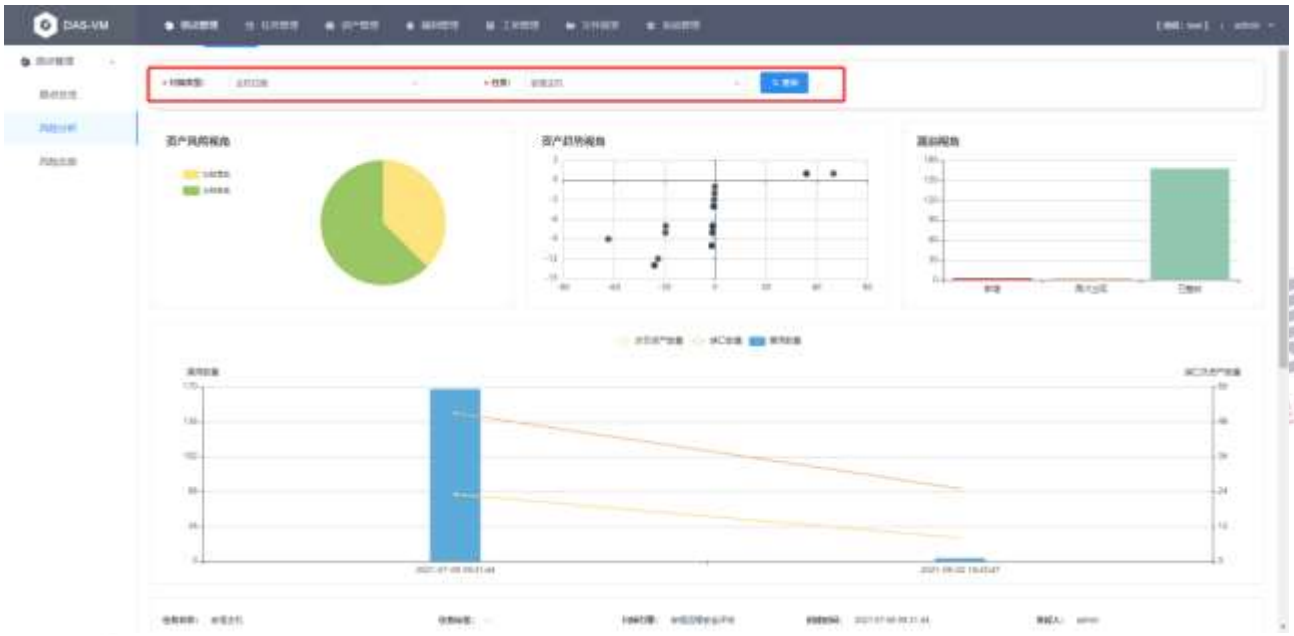
3.1.2.2. 任务维度

任务维度 tab 页主要显示扫描任务结束后指定任务时间段内的对比情况。

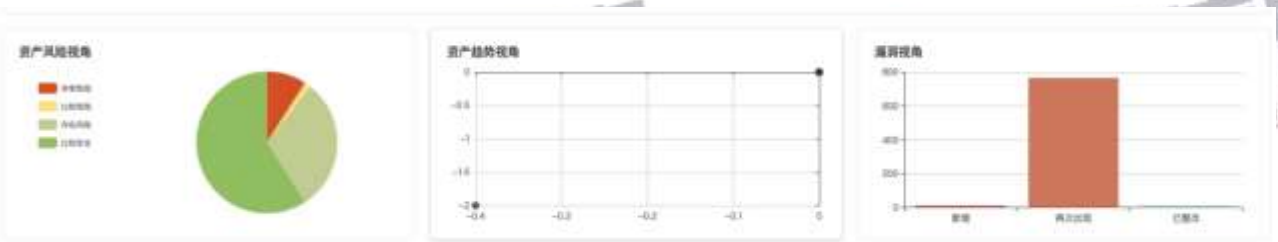
（1） 用户 WEB 登录后，进入[弱点管理 /弱点管理 /风险分析]页面的任务维度 tab 页。



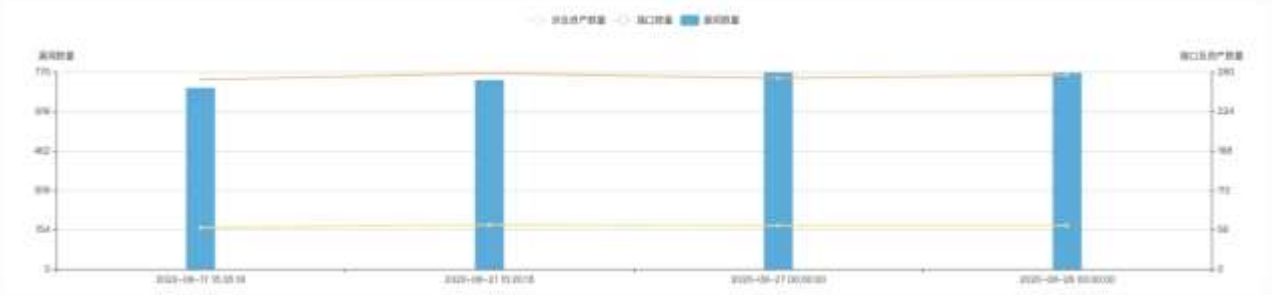
（2） 设置查询条件，扫描类型与任务是必选项，条件设置后，点击<查询>按钮进行查询，默认展示最新子任务信息。



（3） 资产风险视角展示当前选择的任务结果中的资产风险分布，资产趋势视角展示各资产的风险值、漏洞数变化分布，漏洞视角展示再次出现漏洞数量、已修复漏洞数量、新增漏洞数量等信息。



（4） 任务趋势图展示该扫描任务不同子任务间漏洞数量变化、涉及资产资产数量变化和端口数量变化，点击任务趋势图可切换当前子任务。

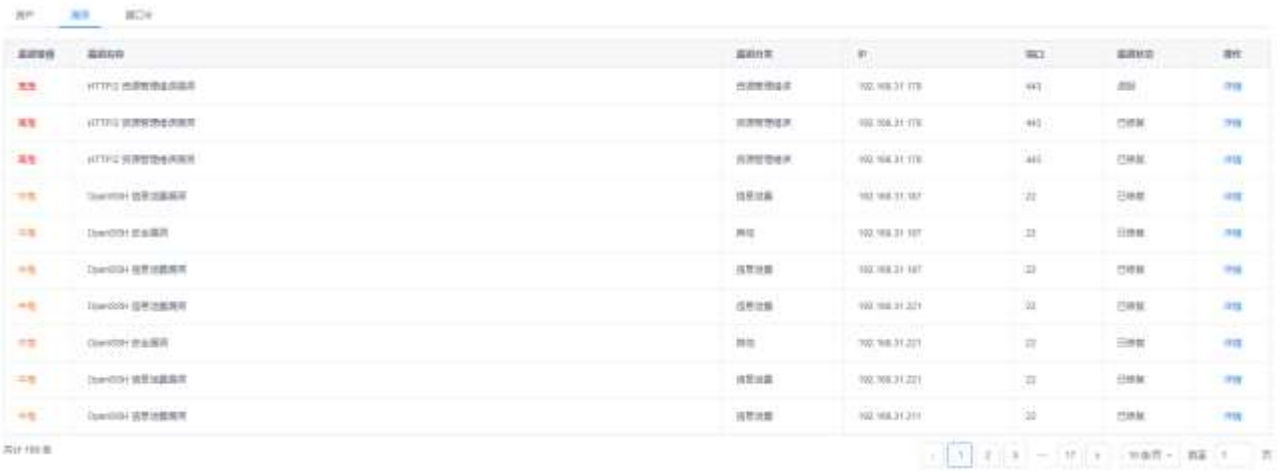


（5） 任务信息栏展示具体任务详细信息。

（6） 点击资产列表，可以查看当前子任务涉及的 IP 地址、端口数量、端口变更、资产存活状态和涉及漏洞数量。

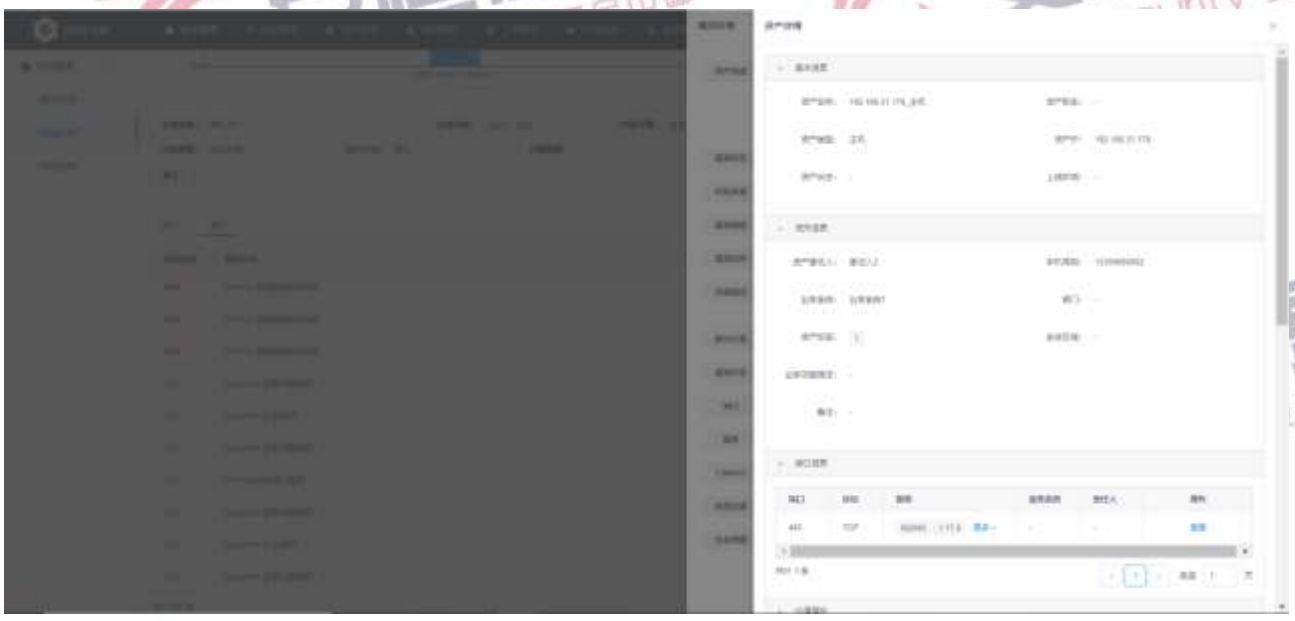
（7） 点击资产列表对应资产的下拉符，可以查看该当前子任务该资产扫描端口的具体信息，包括端口、协议、服务、状态和涉及漏洞数。

（8） 点击漏洞列表，可以查看当前子任务涉及的漏洞信息。



（9） 点击漏洞列表操作列的<详情>按钮，可以查看相应漏洞详情信息。

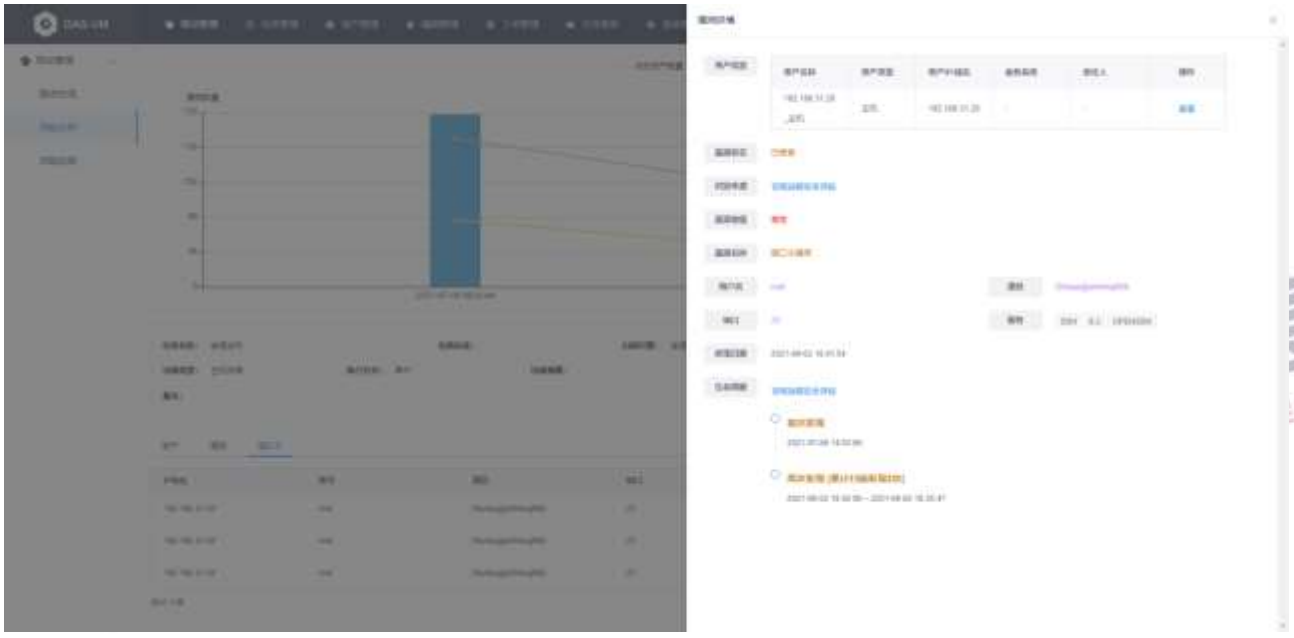
（10） 点击漏洞详情中资产相关信息列表操作列的<详情>按钮，可以查看所属资产的详情信息。



（11） 点击漏洞详情-资产详情中端口信息的<查看>按钮，可以查看所属端口的详情信息。

（12） 存在弱口令漏洞时，可以点击弱口令列表查看相关弱口令漏洞。

（13） 点击弱口令列表中的<详情>按钮，查看具体漏洞信息。

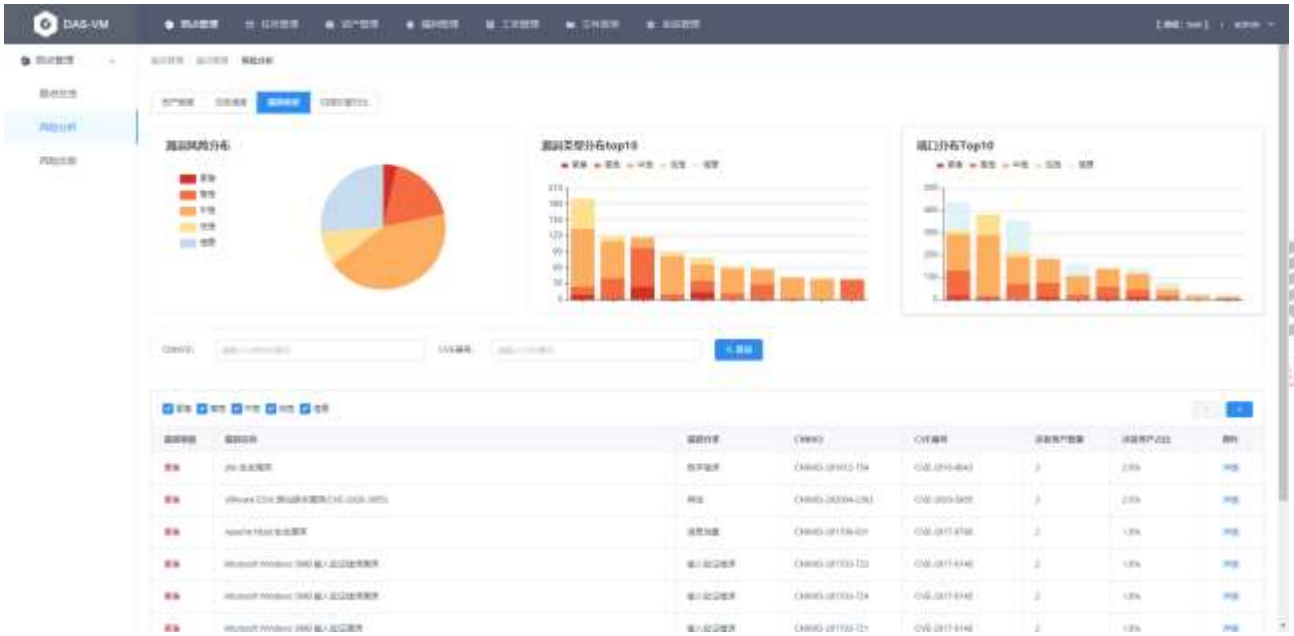


（14） 在弱口令列表-漏洞详情中资产信息，可以点击<查看>按钮，查看具体的资产信息。

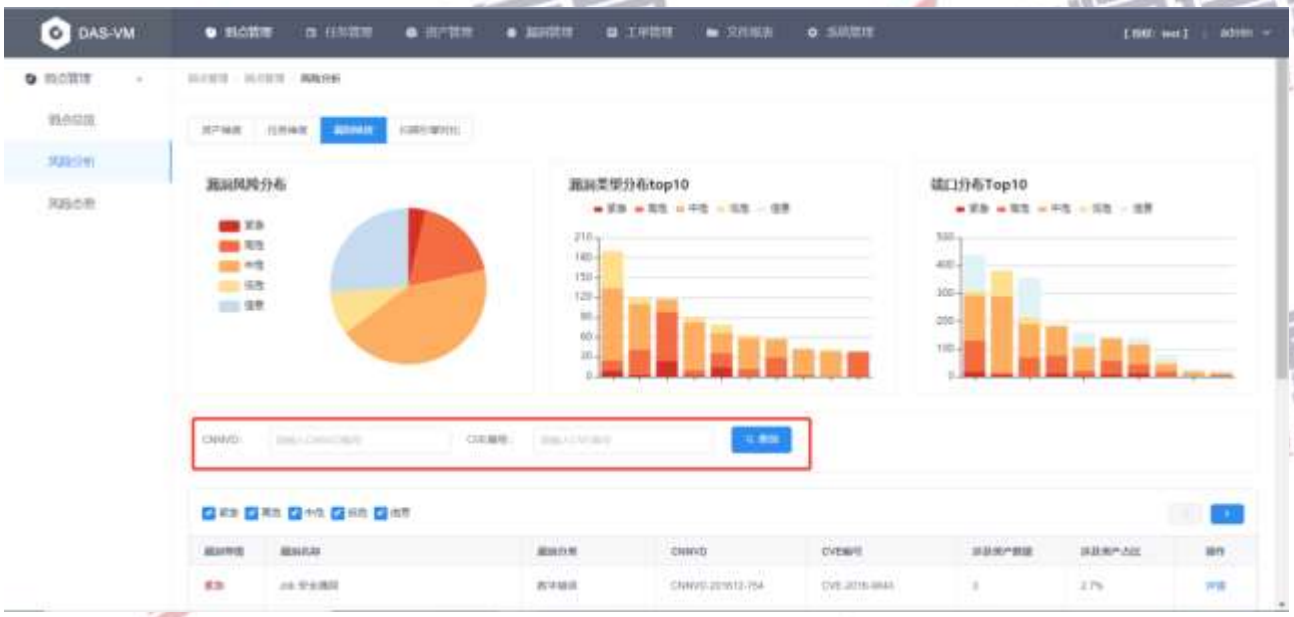
3.1.2.3. 漏洞维度

漏洞维度（指定漏洞）tab 页主要显示平台已添加资产累计扫描发现的主机漏洞信息，并且可以查看漏洞风险分布、漏洞类型分布 TOP10、端口分布 TOP10 等信息。

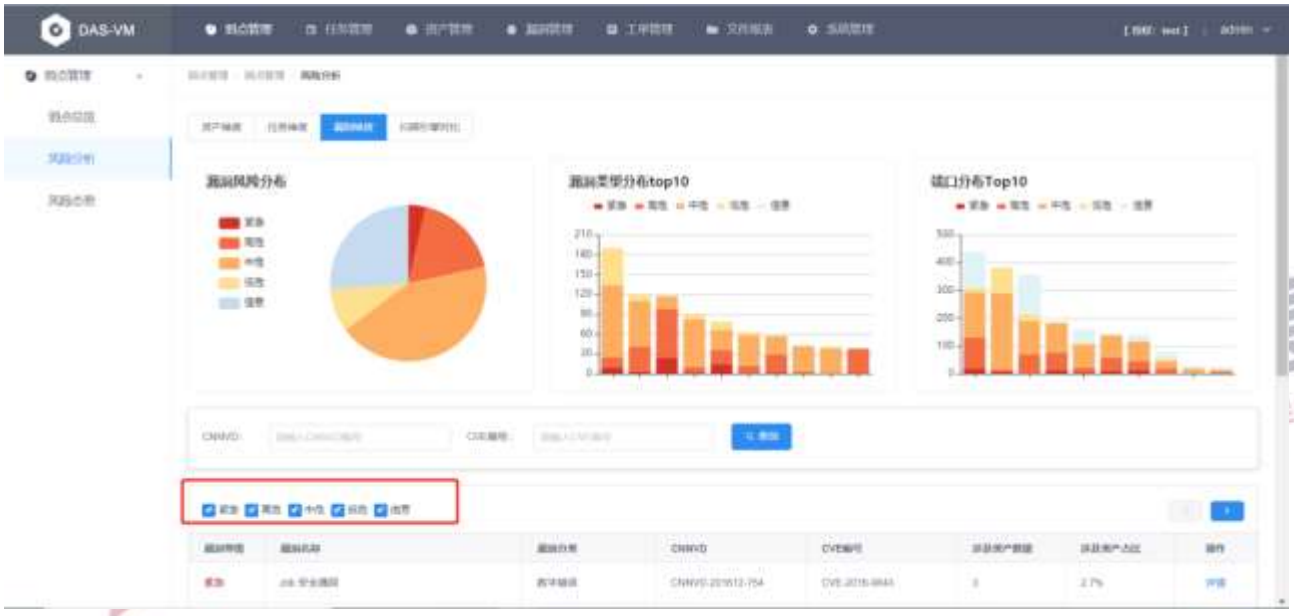
（1） 用户 WEB 登录后，进入[弱点管理 /弱点管理 /风险分析]页面的漏洞维度 tab 页。



（2）设置查询条件：输入 CVE 编号、CNNVD 编号，点击<查询>按钮，进行查询。



（3）勾选漏洞级别可对漏洞进行过滤。



（4） 点击漏洞列表操作列的<详情>按钮，可以查看相应漏洞详情信息。


漏洞详情

资产信息

资产名称	资产类型	资产IP/域名	业务系统	责任人	操作
192.168.31.250_主机	主机	192.168.31.250	-	-	查看
192.168.31.251_主机	主机	192.168.31.251	-	-	查看
192.168.31.245_主机	主机	192.168.31.245	-	-	查看

识别来源 CNNVD | 安恒远程安全评估 | 安恒远程安全评估

漏洞等级 紧急

漏洞名称 zlib 安全漏洞

详细描述 zlib是一个供其他应用程序使用的压缩库，它能够提供数据压缩/解压例程。 zlib 1.2.8版本中的crc32.c文件的'crc32_big'函数存在安全漏洞。攻击者可利用该漏洞造成拒绝服务（应用程序崩溃）。

解决方案 目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接：https://github.com/madler/zlib/commit/d1d577490c15a0c6862473d7576352a9f18ef811

漏洞分类 数字错误

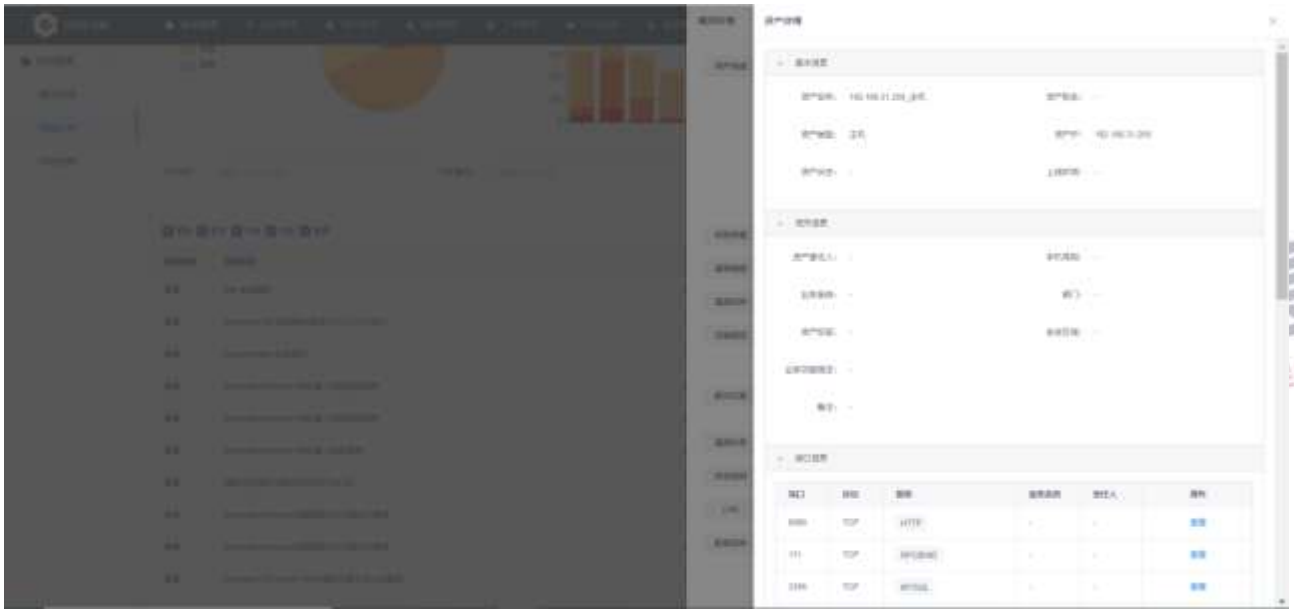
发布时间 2016-12-29　　更新时间 2019-08-07

CVE CVE-2016-9843　　CNNVD CNNVD-201612-754

影响实体

部件	生产厂商	产品名称	产品版本	更新版本	适用版本	界面语言
应用	GNU	ZLIB	1.2.8	-	-	-
操作系统	OPENSUSE	LEAP	42.1	-	-	-

（5）点击漏洞详情中资产相关信息列表操作列的<详情>按钮，可以查看所属资产的详情信息。



3.1.2.4. 扫描引擎对比

扫描引擎对比 tab 页主要显示扫描任务结束后任意 2 个扫描引擎的主机漏洞扫描能力对比与数据分析情况。

（1）用户 WEB 登录后，进入[弱点管理 /弱点管理 /风险分析]页面的扫描引擎 tab 页。

（2）选择对比扫描引擎后，点击<查询>按钮，进行查询，查看主机漏洞扫描能力对比统计图。

（3）选择具体比对扫描引擎后，选填 IP 地址，点击<查询>按钮，进行查询，可查看具体资产两个扫描引擎扫描的漏洞对比结果。

3.1.3. 风险态势

3.1.3.1. 功能介绍

风险态势主要基于资产漏洞等级为紧急、高危、中危的漏洞进行综合的风险的多维度展示。

（1） 用户 WEB 登录后，进入[弱点管理 /弱点管理 /风险态势]页面。

工作统计：

本年已修复漏洞包含所有已修复的紧急、高危、中危漏洞统计。

风险概览：

1. 高危资产：存在紧急、高危、中危漏洞的资产；或资产风险值大于等于 50；
2. 风险漏洞：系统中当前未修复的紧急、高危、中危风险漏洞；
3. 风险系统：风险值大于等于 50 的业务系统；
4. 风险修复率：紧急、高危、中危漏洞的修复率。

风险漏洞趋势：

展示所有漏洞类型的漏洞曲线，分别为主机、基线、弱口令、web、数据库、渗透、误报漏洞。

高危端口排行：

端口涉及紧急、高危、中危漏洞最多的端口 top10。

风险漏洞季度环比：

分别比对本季度与上季度的紧急、高危、中危漏洞，统计时间点定为四个时间点，分别将 2.1 日、5.1 日、8 月 1 日、11 月 1 日零点的漏洞计数为时间点统计。

高风险漏洞：

将漏洞等级为高危、紧急的漏洞统计为高风险漏洞，循环显示前 200 个，排序方式根据漏洞等级、涉及资产数量，统计数量时，仅统计未修复漏洞。

风险系统 Top10：

根据各业务系统的风险评分进行排序，以散点图的形式进行展示风险值最高的十个系统。

风险资产 Top10：

根据各资产的风险评分进行排序，评分相同时，按漏洞数量排序。

4. 任务管理

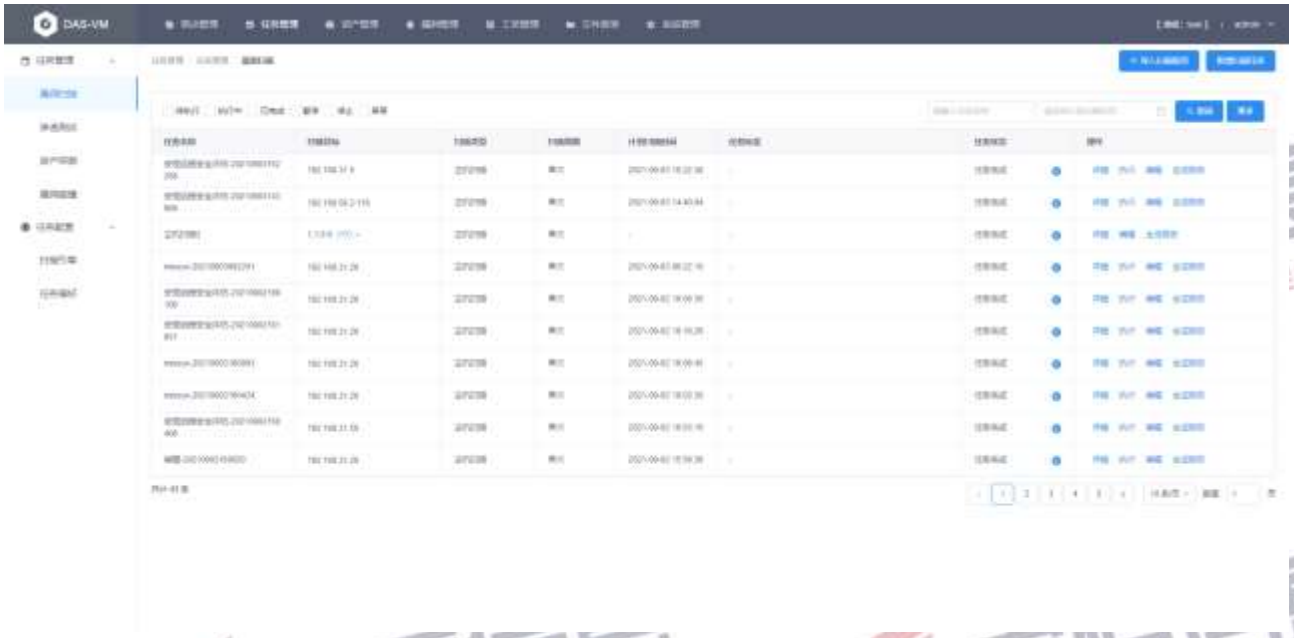
4.1. 任务管理

4.1.1. 漏洞扫描

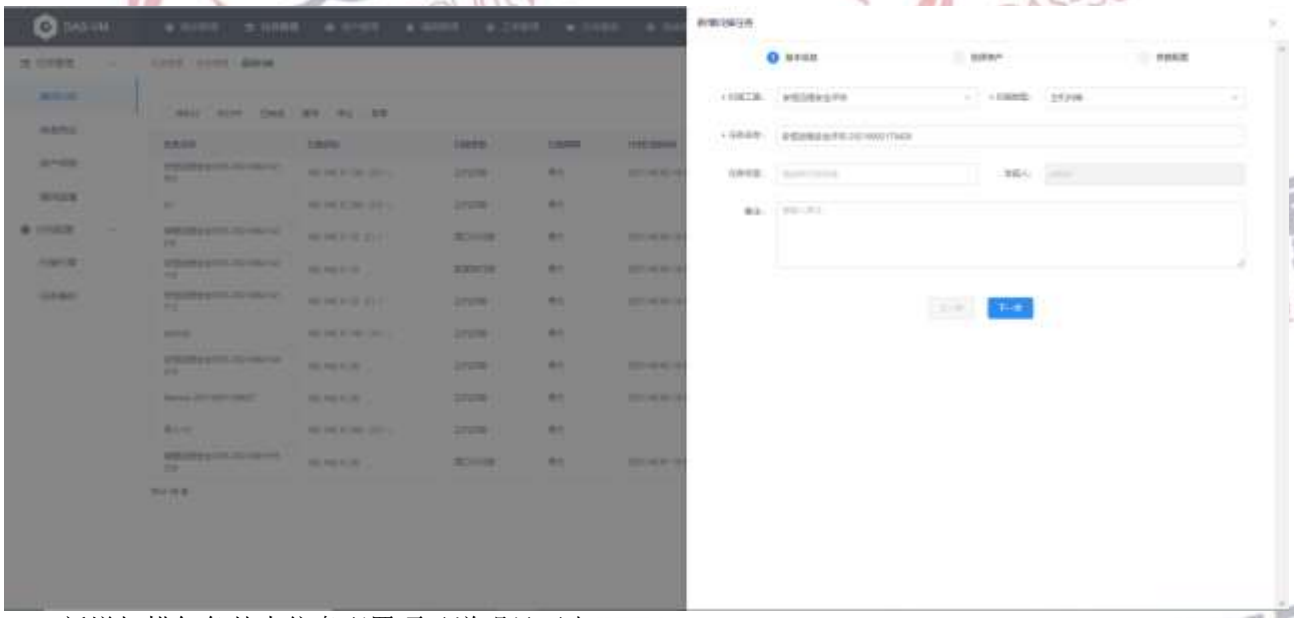
漏洞扫描可以查看扫描引擎的漏洞扫描任务下发与简单的任务结果，具体包括以下几个方面的内容：扫描任务创建和执行、扫描进度查看、扫描结果查看。

4.1.1.1. 扫描任务新增

（1） 用户 WEB 登录后，进入[任务管理/任务管理/漏洞扫描]页面。



（2） 点击右上角的<新增扫描任务>按钮，弹出新增扫描任务窗口，默认进入基本信息页面，选择扫描工具、扫描类型和任务标签，输入任务名称和备注。

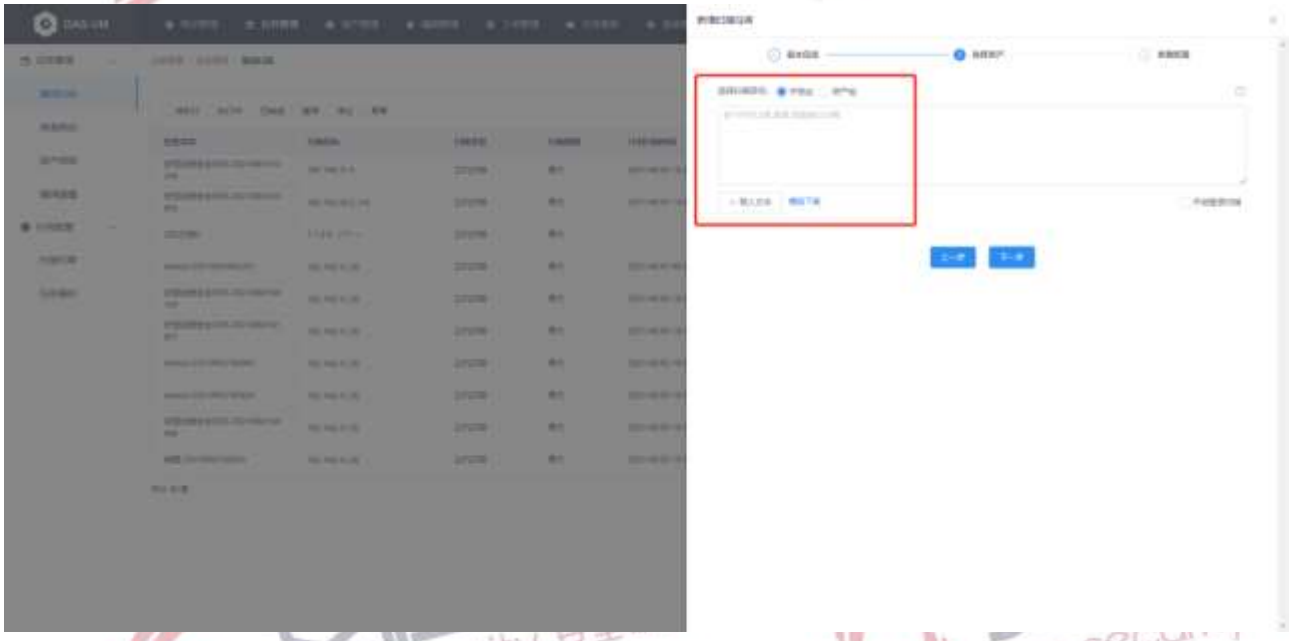


新增扫描任务基本信息配置项及说明见下表：

配置项	说明
扫描工具	必填项。选择扫描工具，可选扫描引擎管理列表中已添加成功的扫描引擎。
扫描类型	必填项。安恒远程安全评估扫描引擎可选择主机扫描、web 扫描、基线扫描、弱口令扫描、数据库扫描，绿盟远程安全评估扫描引擎可选择主机扫描、基线扫描、弱口令扫描，Nessus 扫描引擎可选择主机扫描。

任务名称	必填项。新增扫描任务的任务名称。
任务标签	选填项。选择任务标签，将扫描任务归类到对应标签下。可在任务标签选择框内点击添加标签，选择任务标签分类，输入标签名称快速完成任务标签添加，所添加的任务标签重要性为 1。当无任务标签分类时，快速添加任务标签时默认增加名称为“任务”、重要性为 1 的任务标签分类。
发起人	必填项，置灰。默认创建扫描任务的发起人，即当前登录用户。
备注	选填项。新增扫描任务的注解说明。

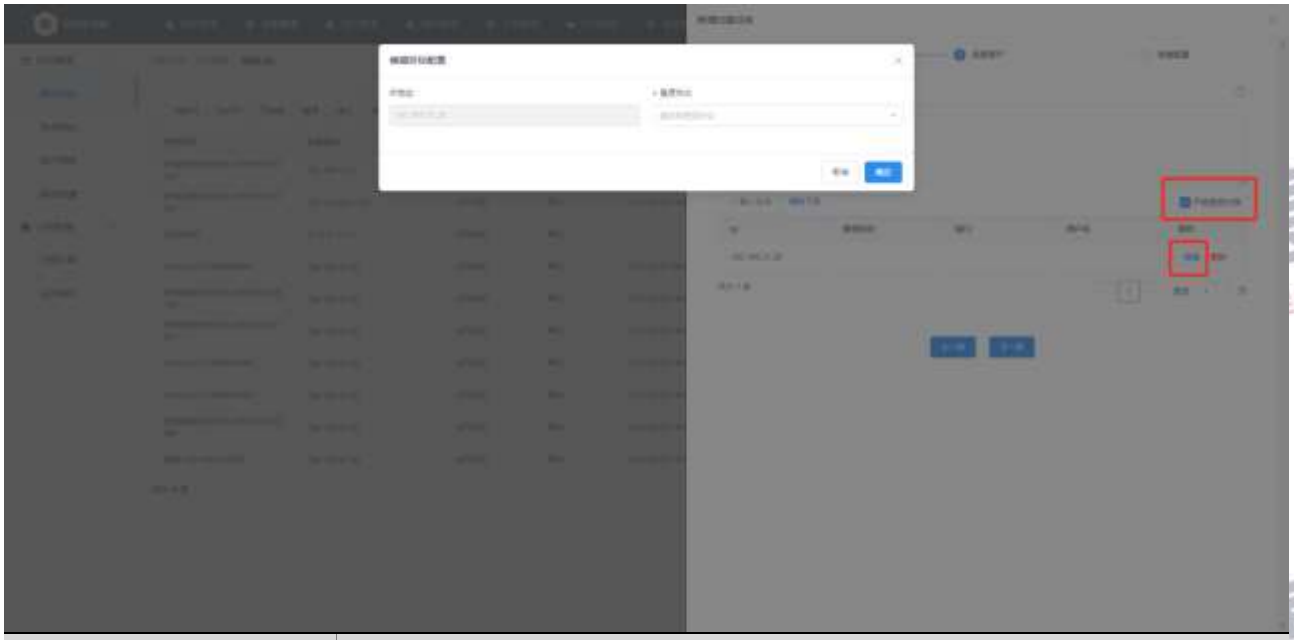
（3）点击<下一步>按钮进入选择资产页面，输入扫描目标，可以输入 IP 地址₩域名地址或搜索资产组进行选择,也可通过点击<模板下载>按钮下载模板，编辑后点击<导入文件>按钮批量导入。



新增扫描任务选择资产配置项及说明见下表：

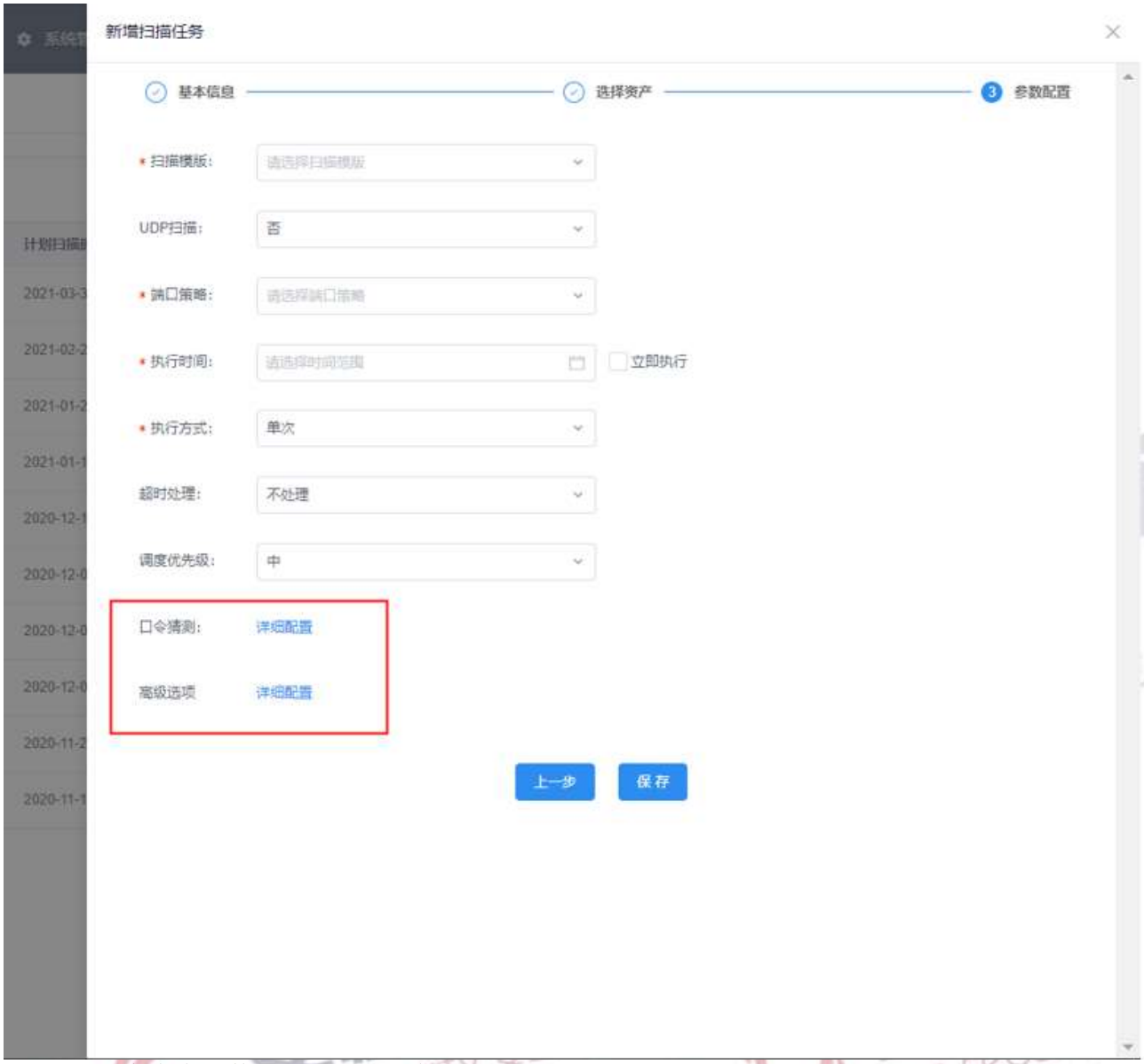
配置项	说明
IP 地址	可以添加单个 IP 地址或 IP 段，如：192.168.0.1 或 192.168.1.1-254。
域名地址	创建安恒远程安全评估的 WEB 扫描任务特有的扫描目标，可以添加单个或多个域名地址，如 http://192.168.0.1。
资产组	可以直接选择平台已添加的资产组或单个资产，可通过名称搜索具体资产。
导入文件	可通过导入 excel 文件批量导入 IP 地址等扫描目标。
?	提示图标，可以显示扫描目标格式示例。

创建安恒远程安全评估主机任务时，可以开启登录扫描，首先通过导入文件输入 IP 地址，然后可以编辑和删除相关 IP，其中点击<编辑>按钮进入编辑目标配置可以选择登陆协议。



配置项	说明
IP 地址	已经选择的 IP 地址。
登录协议	必填项。可选择的协议类型有 SMB、SSH、SNMP。

（4）点击<下一步>按钮进入参数配置页面，选择扫描模板、执行时间、是否立即执行、执行方式、超时处理、口令猜测、调度优先级等内容，点击<保存>按钮 ，扫描任务创建完成。

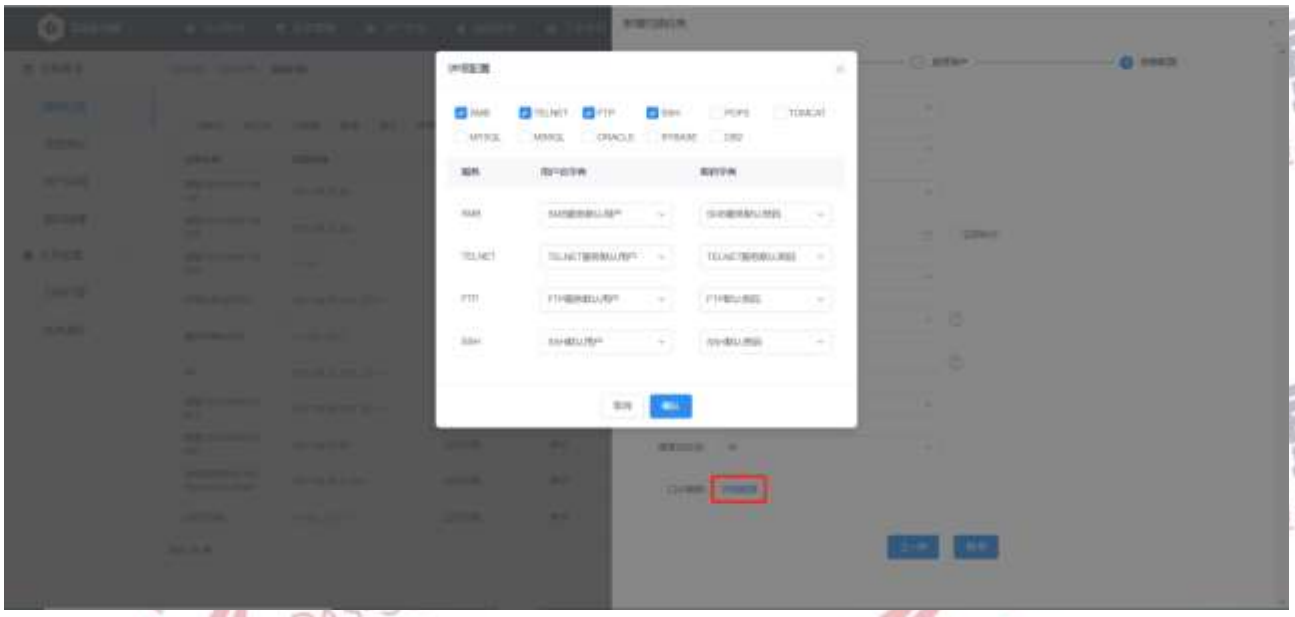


新增扫描任务参数配置配置项及说明见下表：

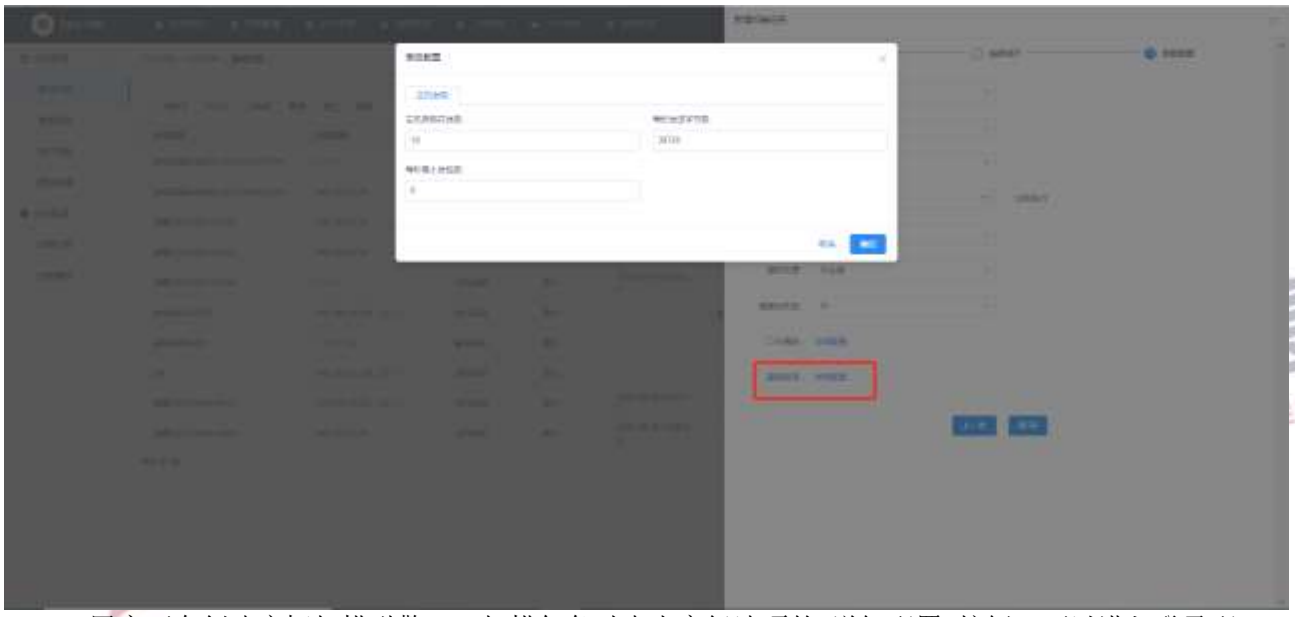
配置项	说明
扫描模板	必填项。发往扫描引擎的扫描任务执行模板。
执行时间	必填项。扫描引擎正式开始扫描的时间。
立即执行	勾选项。扫描引擎执行是否立即执行一次。
执行方式	必填项。扫描引擎执行扫描的周期，可选择：单次、每天、每周、每月、每年，与执行时间组合搭配。
超时处理	选填项。扫描任务超时对扫描任务的处理方式，可选项有：不处理、暂停、停止。

超时时间	选填项。超时处理方式选择暂停或停止时，此选项才会被激活，可选择超时时间：10 小时、5 小时、2 小时。
调度优先级	选填项。扫描任务优先级，可选：高、中、低。
扫描深度	必选项。仅绿盟扫描引擎创建扫描任务时展示该配置，可选深度值 1-5，深度值越大，插件扫描获取的信息可能就越多。
插件超时限制	必填项。仅绿盟扫描引擎创建扫描任务时展示该配置，可选超时限制范围为 1-300 秒，单个插件在指定插件超时限制时间内如果未正常结束将会被调入引擎终止。
口令猜测	安恒远程安全评估的主机、弱口令扫描任务，以及绿盟远程安全评估的主机、弱口令扫描任务的配置项，可以配置口令的详细配置。
高级选项	安恒远程安全评估的 WEB、弱口令扫描任务的配置项，可以配置详细的高级配置。

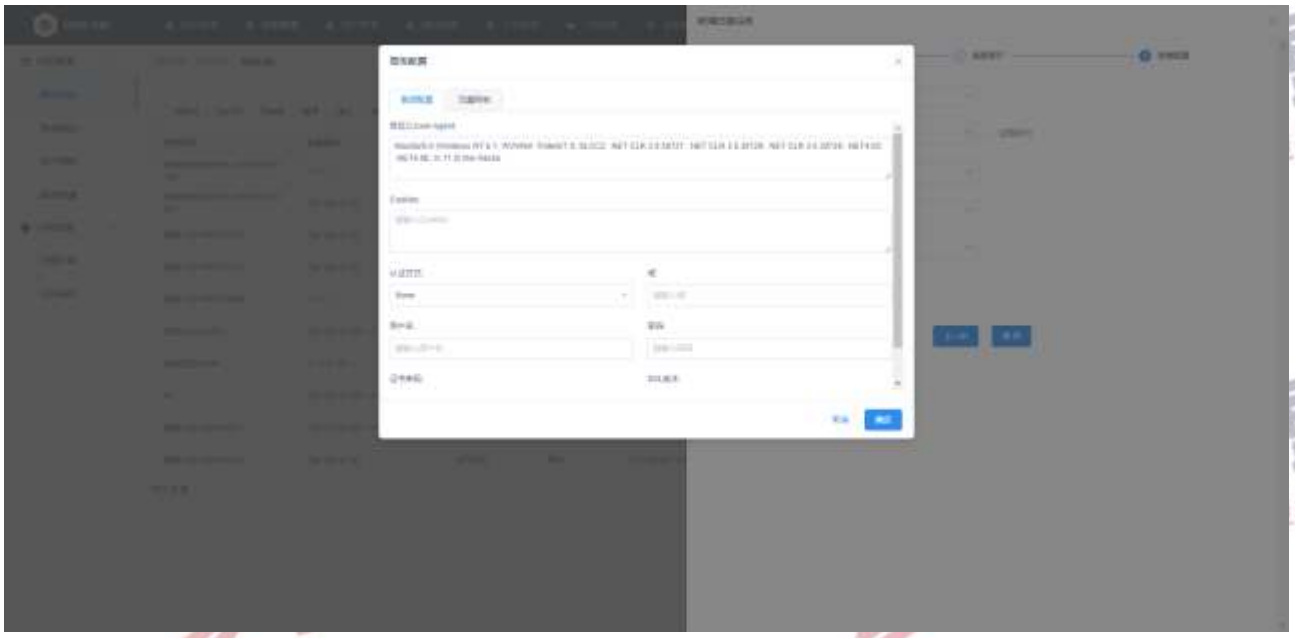
（5） 点击口令猜测栏的<详细配置>按钮，可以勾选要进行弱口令扫描的相应服务项并配置对应的用户名字典和密码字典，其中 SNMP 服务无用户名字典。



（6） 点击高级选项栏的<详细配置>按钮，可以进行相关高级选项配置。



用户可在创建安恒扫描引擎 WEB 扫描任务时点击高级选项的<详细配置>按钮，可以进入登录配置页面进行登录扫描的参数配置。



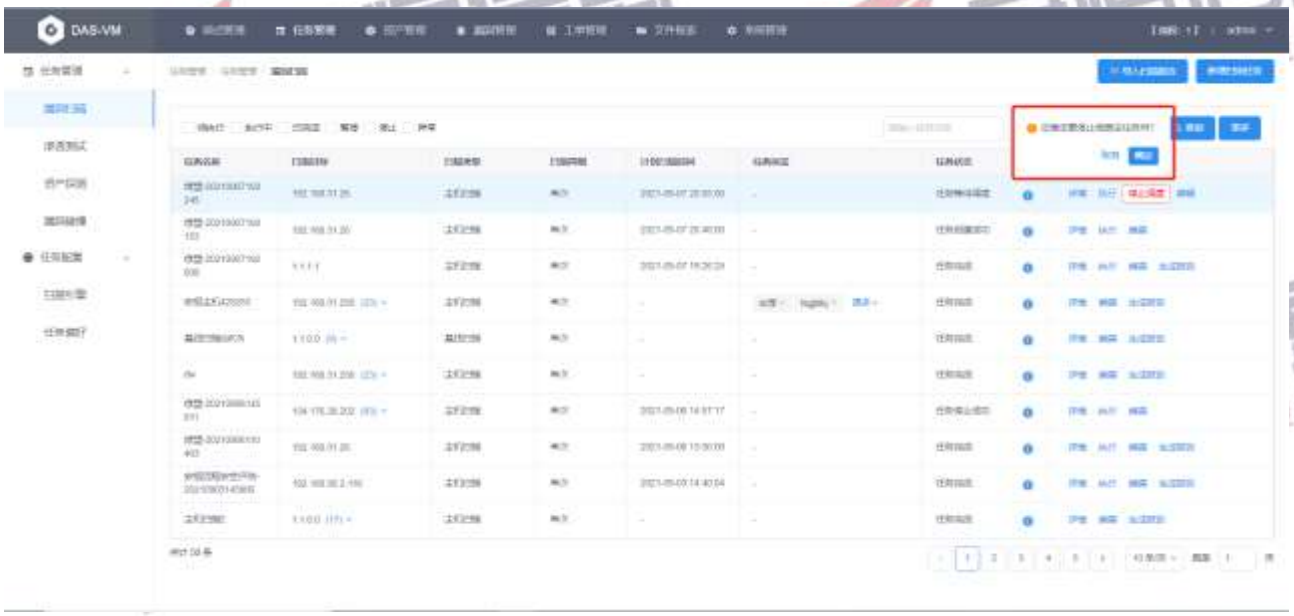
详细配置参数如下：

配置项	说明
自定义 User-Agent	登陆配置的自定义 User-Agent。
Cookies	选填项。登陆配置的 Cookies。
认证方式	登陆配置的认证方式，可选项有 AnySate、Basic 等方式。
域	选填项。登陆配置的域名。
用户名	选填项。登陆配置的用户名。

密码	选填项。登陆配置的密码。
证书密码	选填项。登陆配置的证书密码。
SSL 版本	选填项。登陆配置的 SSL 版本。
最大接受速率	流量限制的最大接受速率，单位为千字节/秒。
最大发送速率	流量限制的最大发送速率，单位为千字节/秒。
最大并发连接数	流量限制的最大并发连接数。
每秒最大发送请求数	流量限制的每秒最大发送请求数。
启用智能流控	流量限制的智能流控，可以选择开启或者关闭。

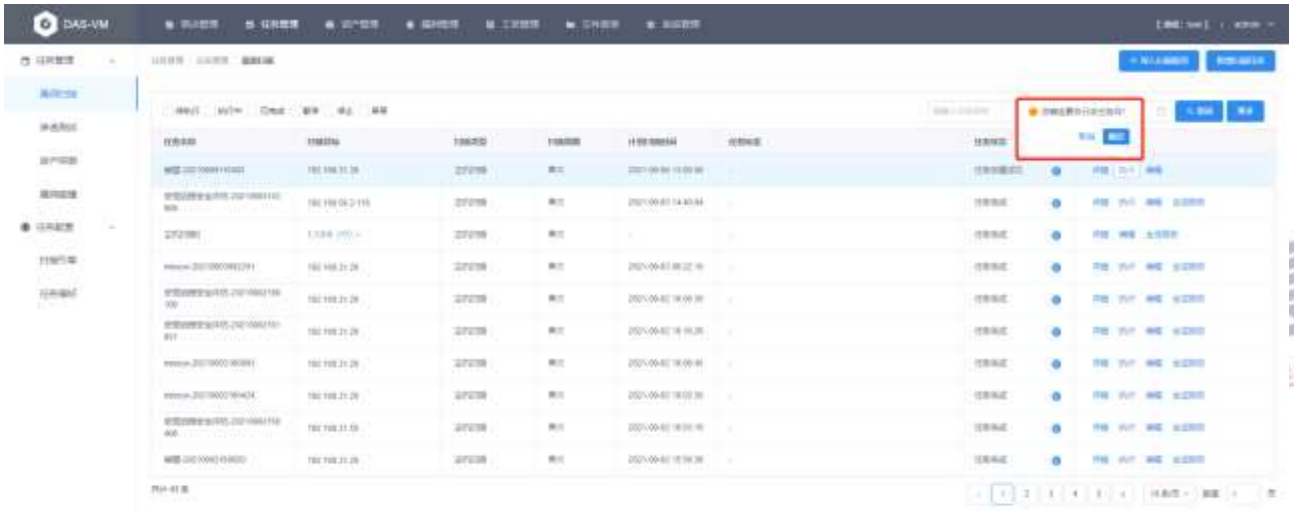
4.1.1.2. 扫描任务停止调度

（1） 当扫描任务处于等待调度状态时，点击任务列表中的<停止调度>按钮并确定，可停止调度扫描任务。

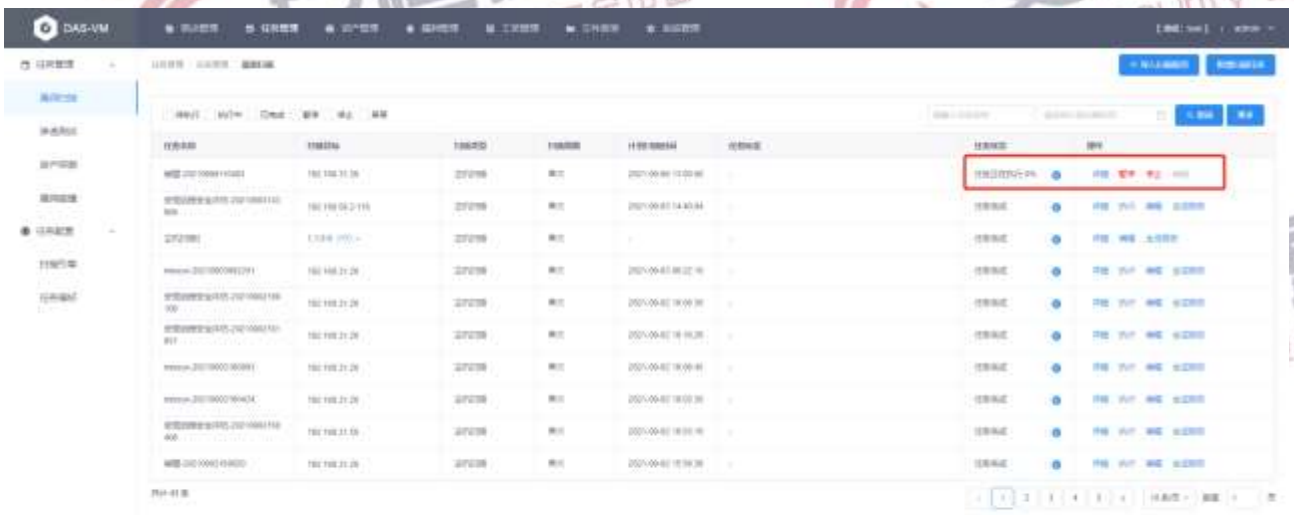


4.1.1.3. 扫描任务执行

（1） 点击任务列表中的<执行>按钮并确定，可立即执行一次对应的扫描任务。

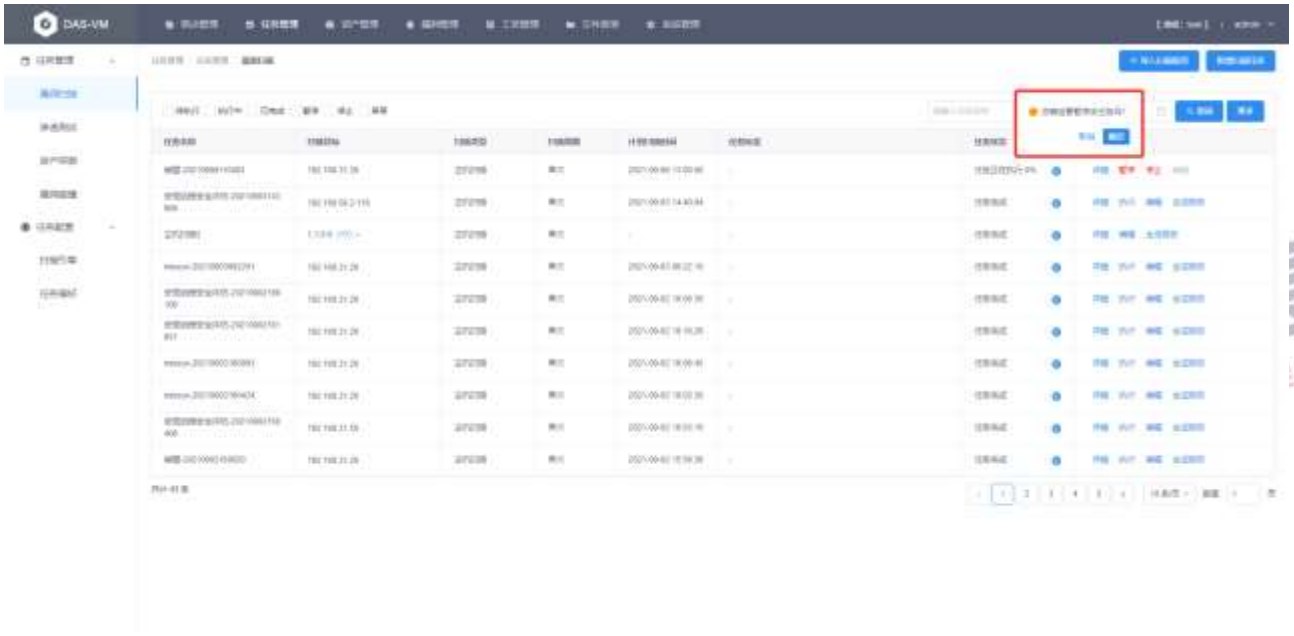


（2）任务开始执行后，右侧操作栏按钮变为<详情>、<暂停>、<停止>和<编辑>，可以查看任务详情或对任务进行暂停、停止等操作，<编辑>按钮置灰。

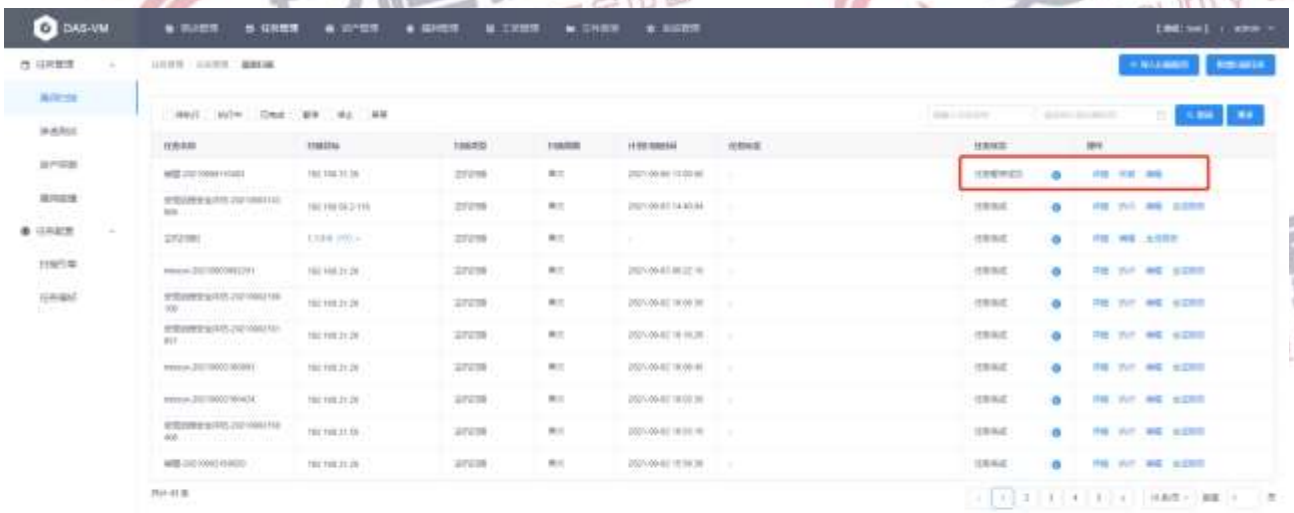


4.1.1.4. 扫描任务暂停与恢复

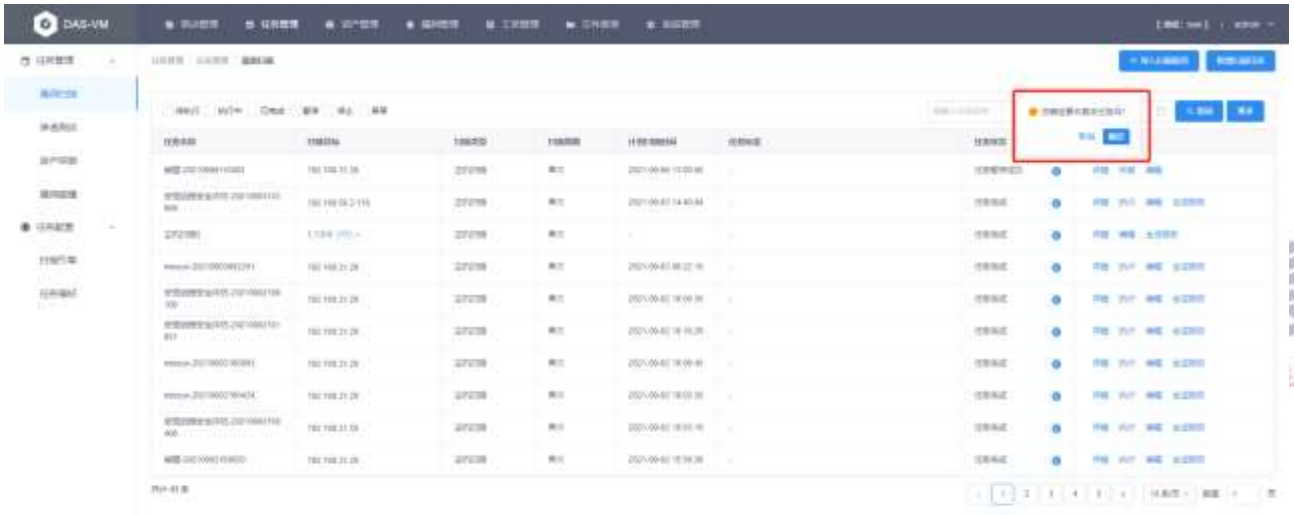
（1） 点击任务列表中的<暂停>按钮并确定，可暂停正在执行的扫描任务。



（2）暂停任务成功后，对应任务状态变更为任务暂停成功，右侧操作栏按钮变为<详情>、<恢复>和<编辑>。

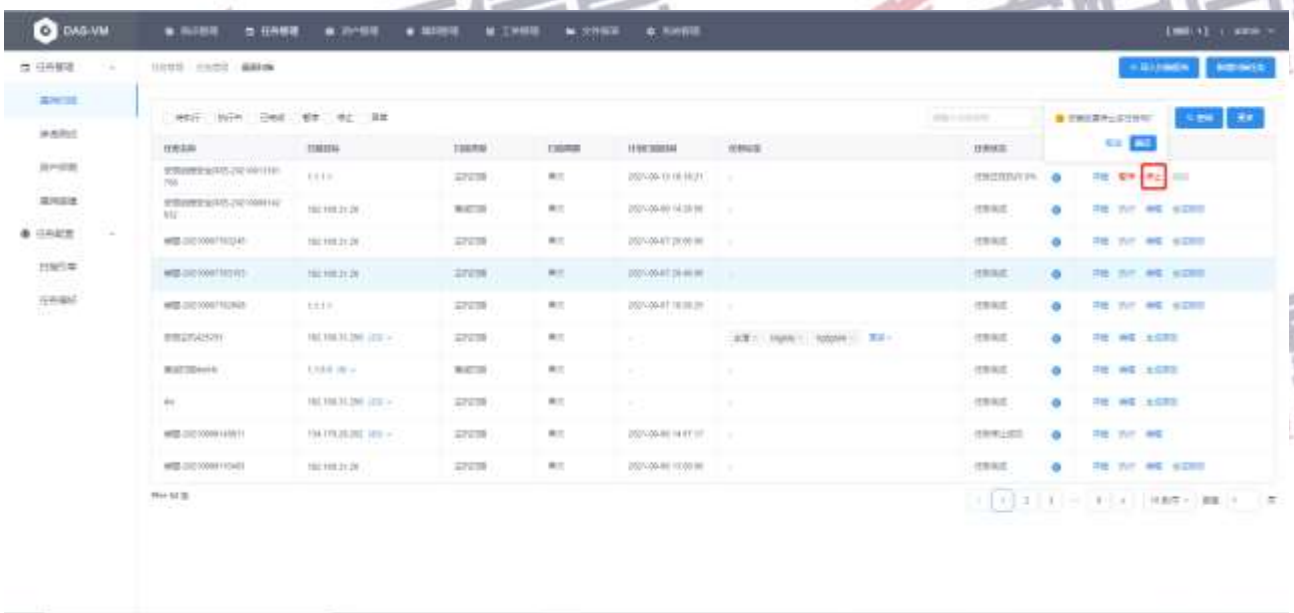


（3）点击任务列表中的<恢复>按钮并确定，可恢复暂停中的扫描任务，使其继续执行。

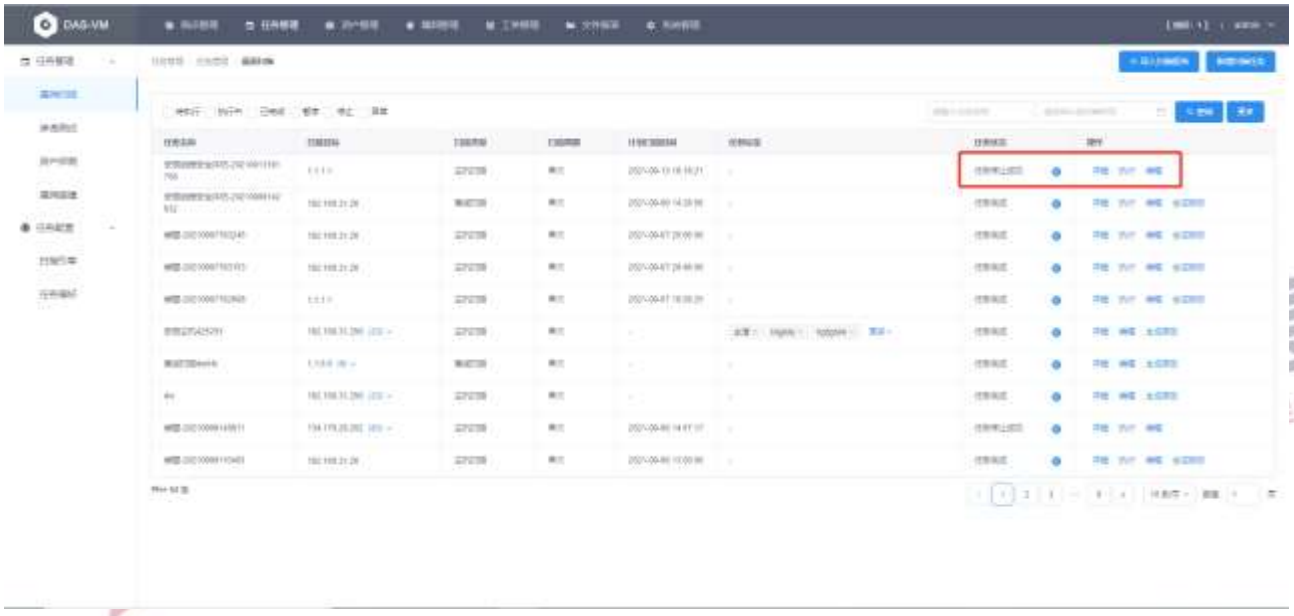


4.1.1.5. 扫描任务停止

（1） 点击任务列表中的<停止>按钮并确定，可停止正在执行的扫描任务。

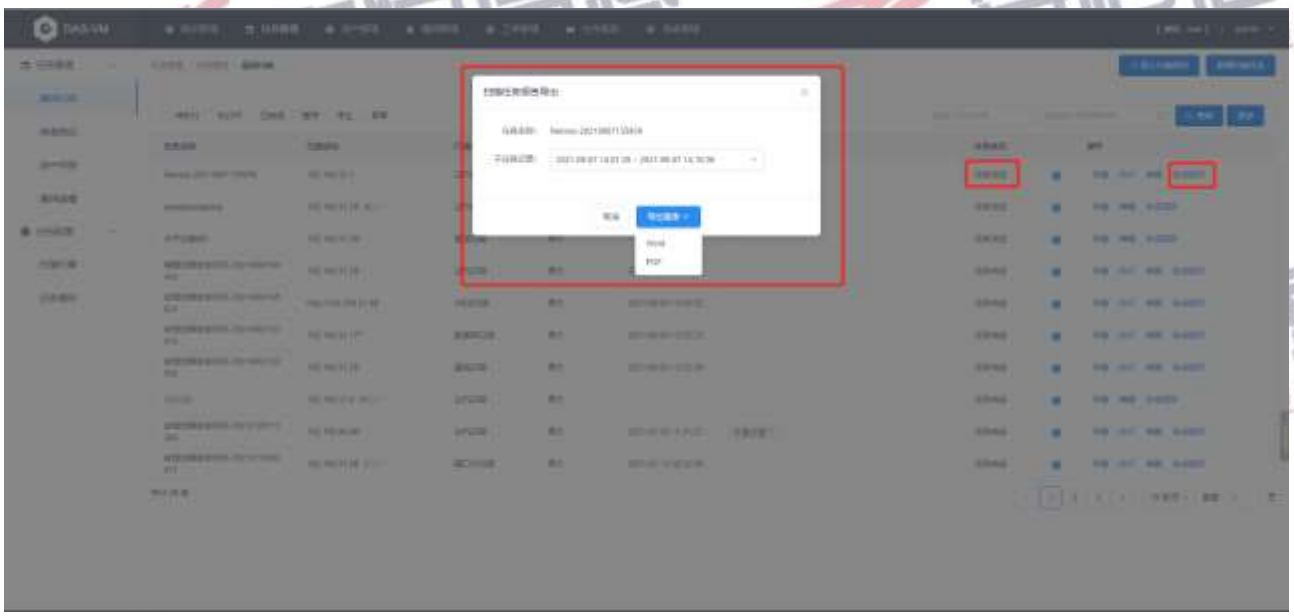


（2）停止任务成功后，对应任务状态变更为任务停止成功，右侧操作列按钮变为<详情>、<执行>和<编辑>。

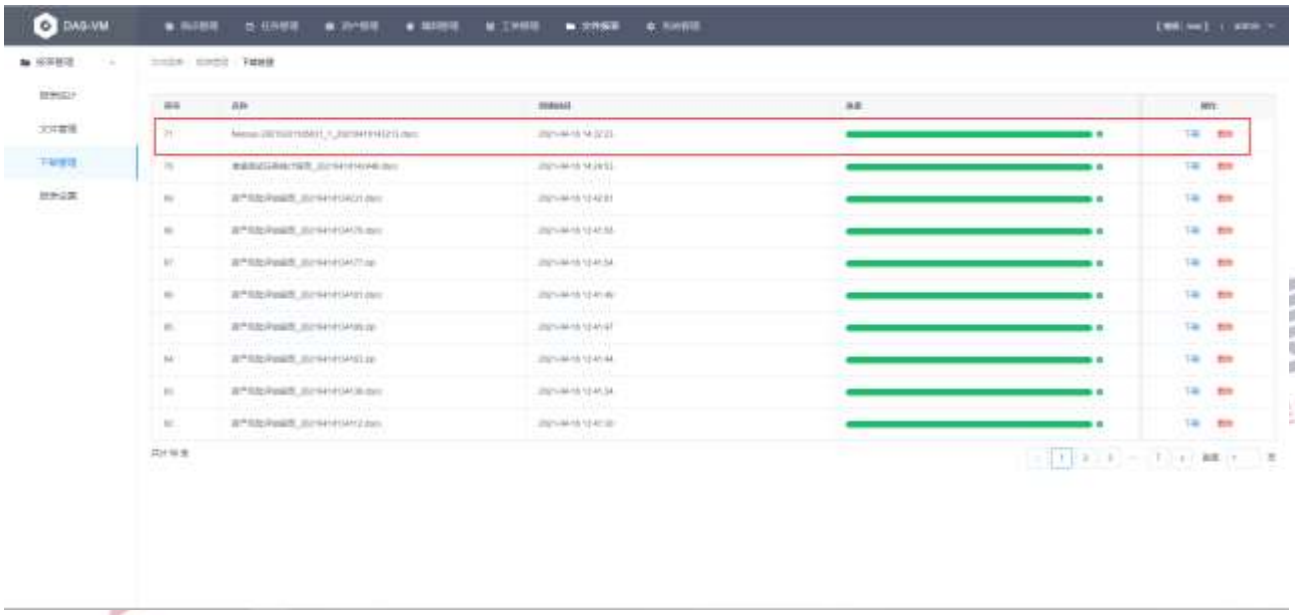


4.1.1.6. 生成扫描任务报告

（1） 扫描任务完成后，点击<生成报告>按钮，选择对应起止时间的子任务记录，点击<导出报表>按钮，下拉展开导出格式选项，选择导出格式 Word 或 PDF，可以导出选中子任务指定格式的统计报表。

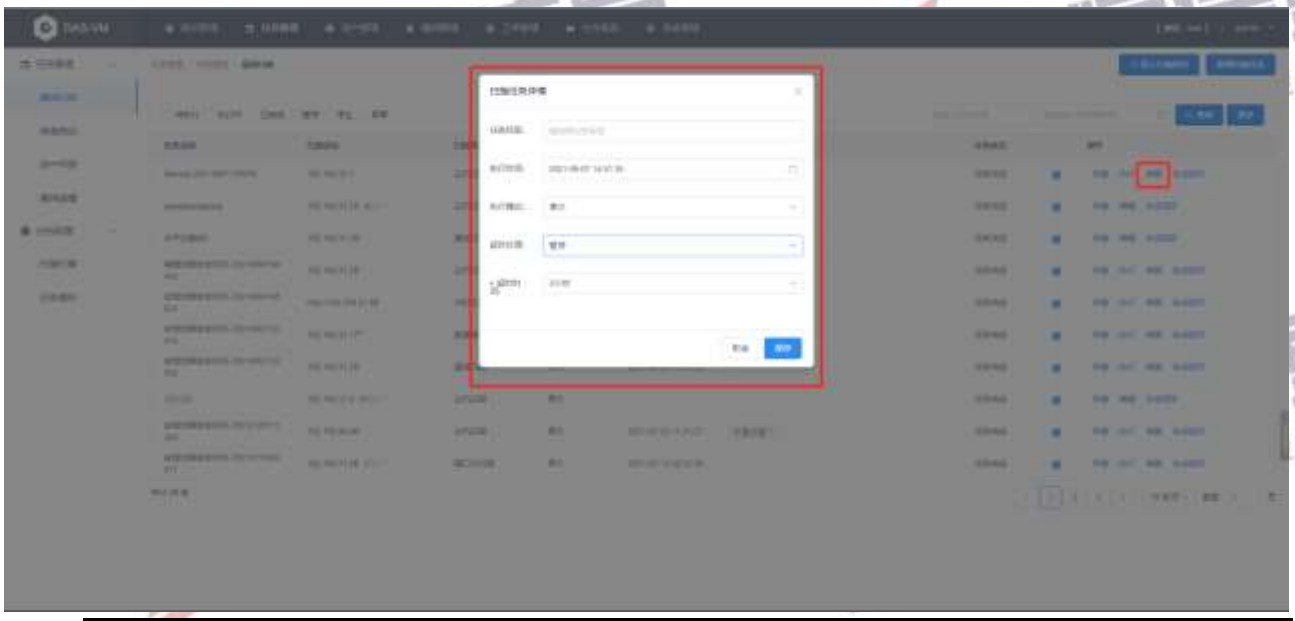


（2）[文件报表/报表管理 /下载管理]页面新增一条导出记录，待进度条达到 100%转绿后，点击<下载>按钮，即可下载导出的扫描任务统计报告。



4.1.1.7. 扫描任务编辑

（1） 点击任务列表中的<编辑>按钮，可以在扫描任务详情编辑页面修改扫描任务的任务标签、执行时间、执行方式、超时处理和超时时间。

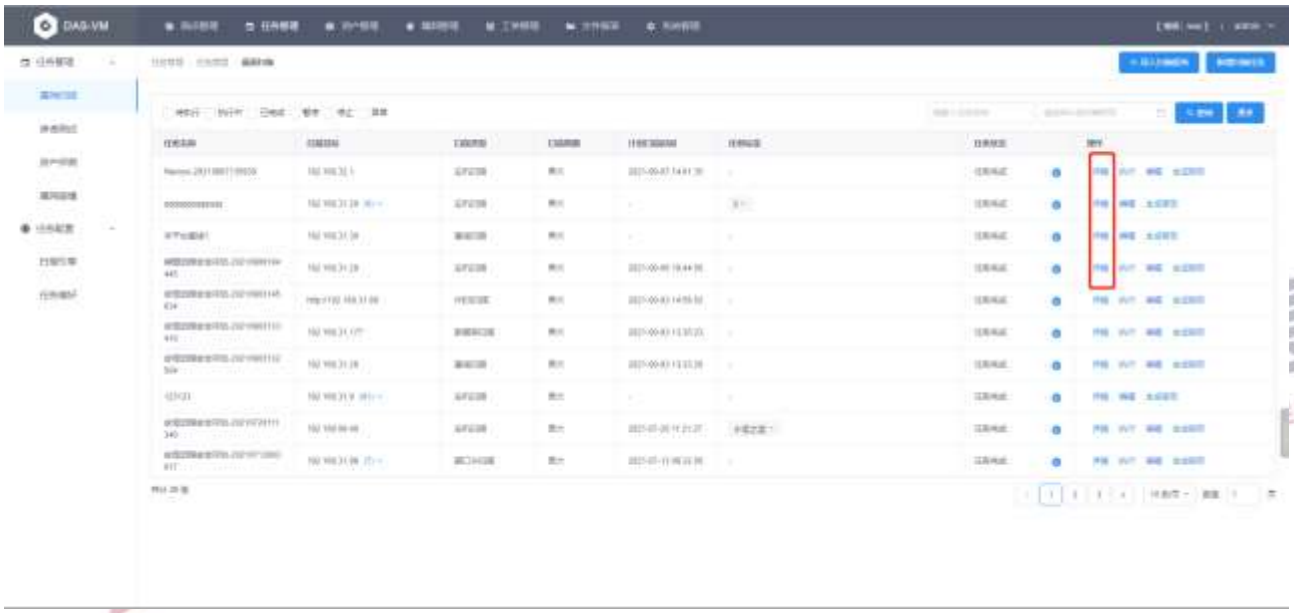


注意

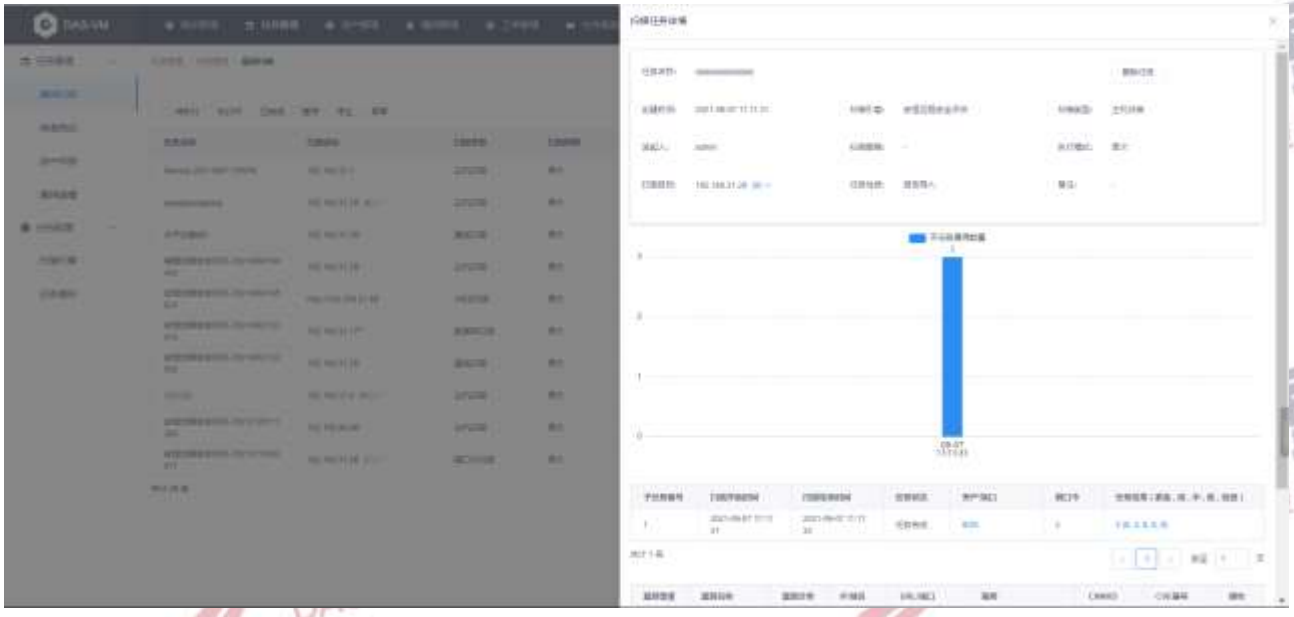
<编辑>按钮只能修改扫描任务的任务标签、执行时间、执行方式、超时处理、超时时间。

4.1.1.8. 扫描任务详情

（1） 点击扫描任务列表中的<详情>按钮，可以查看该任务的任务详情。

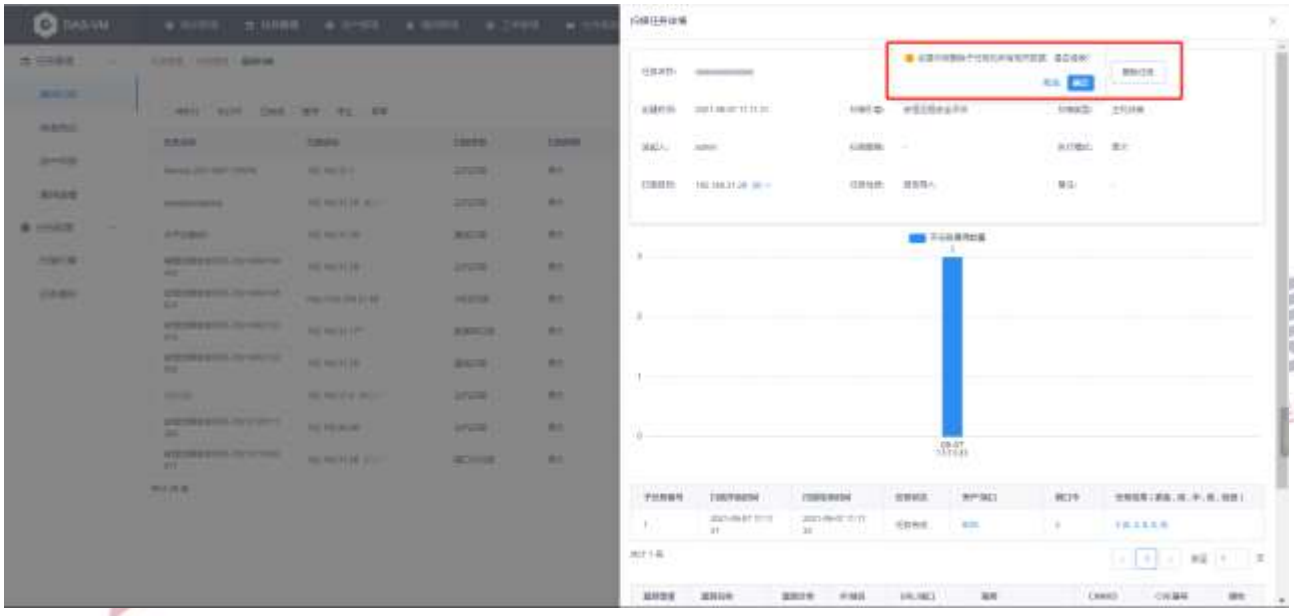


（2） 扫描任务详情可查看该任务的任务名称、扫描策略、扫描类型、扫描工具等任务信息以及各子任务扫描结果。



4.1.1.9. 扫描任务删除

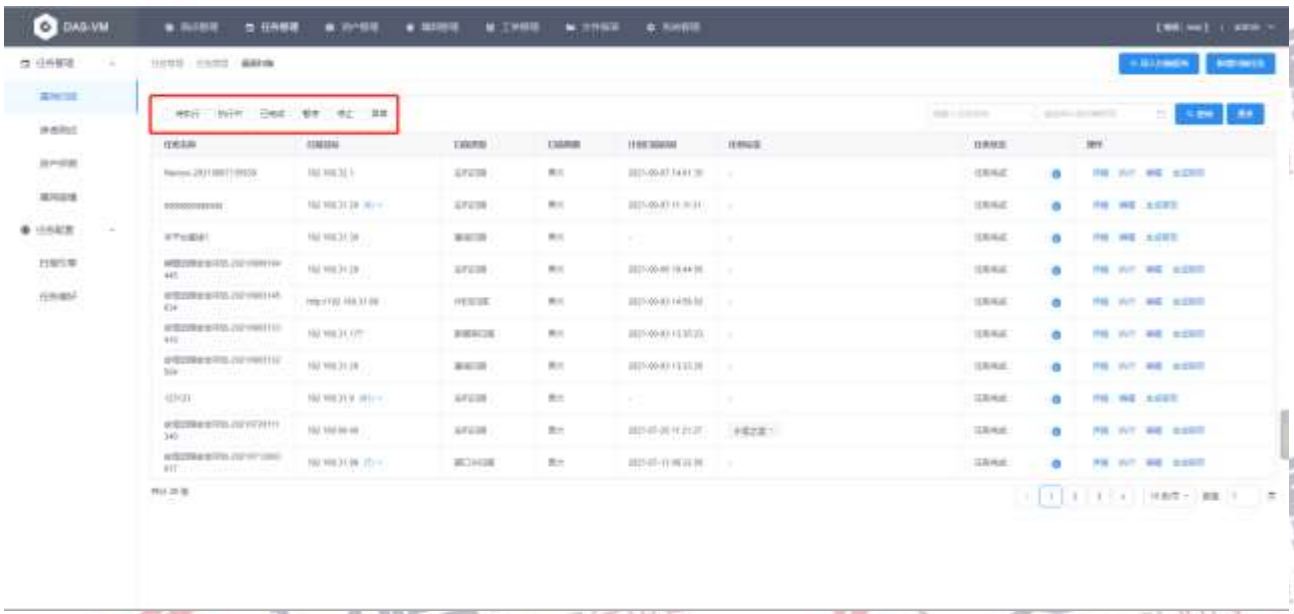
（1） 点击扫描任务详情的右上角<删除任务>按钮，点击<确定>，可删除对应的扫描任务。



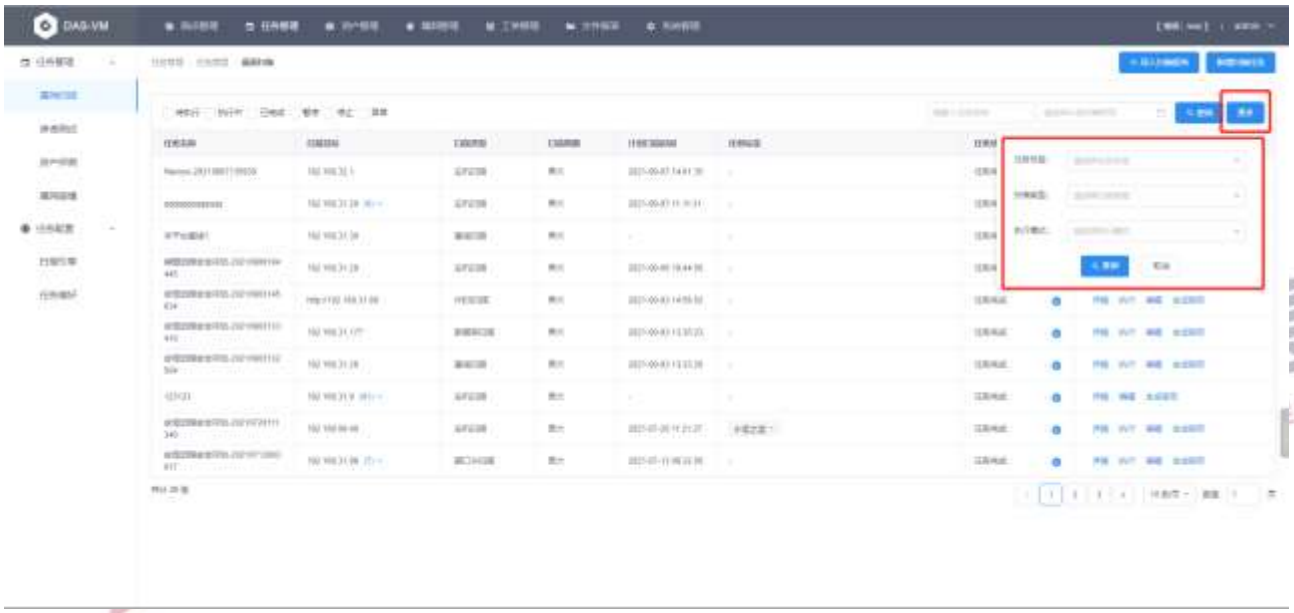
4.1.1.10. 扫描任务查询

（1） 勾选页面中的任务完成情况：待执行、执行中、已完成、暂停、停止、异常，即可进行相应的扫描任务查询，具体完成情况细分如下：

- 待执行：当前尚未开始执行或正在等待调度的任务。
- 执行中：当前正在执行的扫描任务。
- 已完成：已经执行完成的扫描任务。
- 暂停：执行过程中被暂停的扫描任务。
- 停止：执行过程中被停止的扫描任务。
- 异常：执行过程中出现异常的扫描任务。



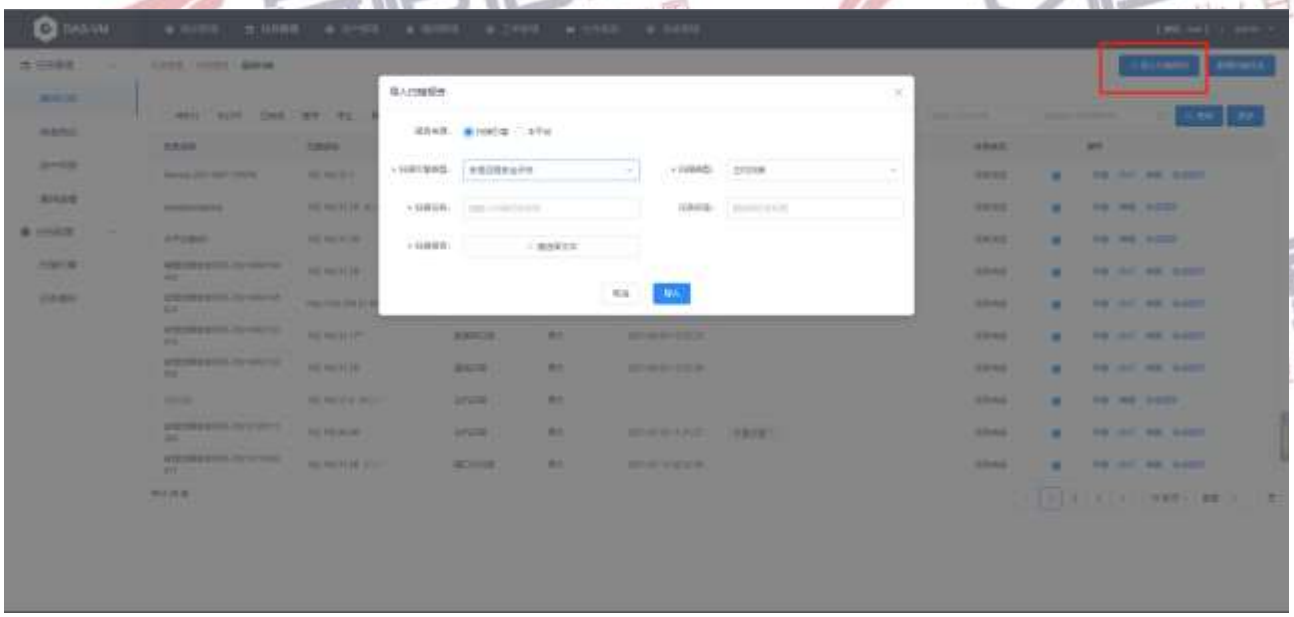
（2） 选择查询时间、任务名称后，点击<查询>按钮进行任务查询，也可点击<更多>按钮，选择更多的查询条件，如：任务标签、扫描类型、执行方式。



4.1.1.11. 扫描报告导入

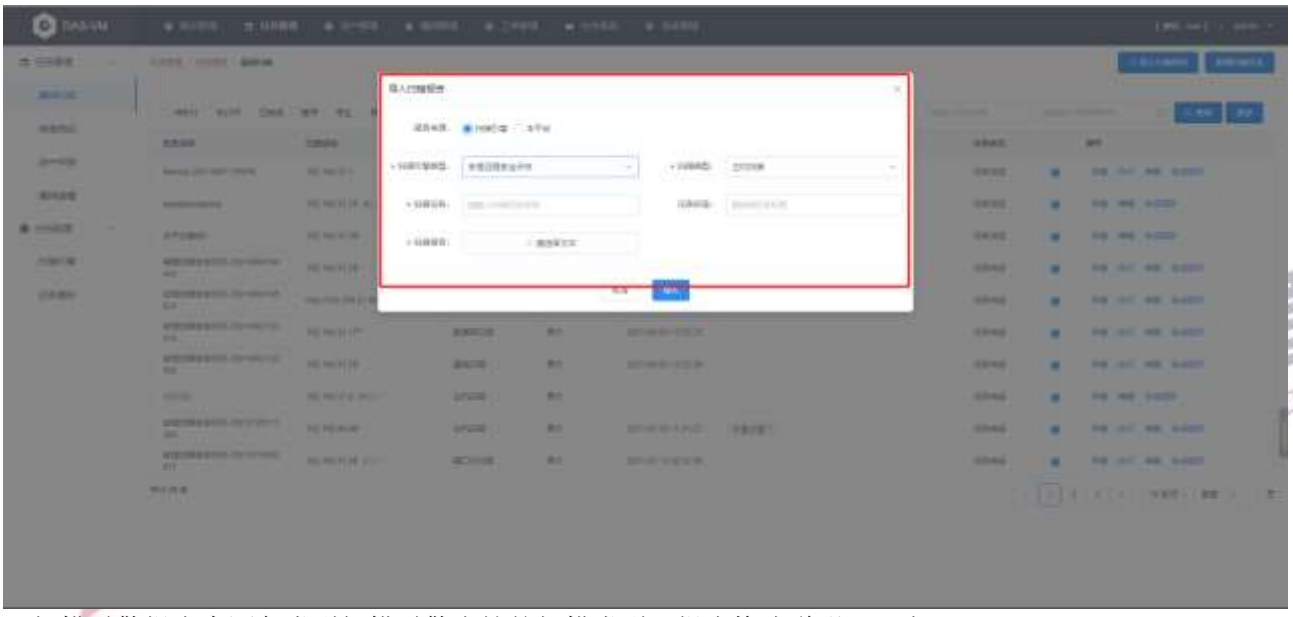
离线扫描报告导入时系统会自动生成一个对应的扫描任务，任务状态为已完成。该类任务不能下发给扫描引擎。支持的扫描报告格式为绿盟、安恒扫描引擎的 xml 格式扫描报告和对应 excel 模板格式的扫描报告。

（1） 点击右上角的<导入扫描报告>按钮，弹出导入扫描报告窗口。



（2）选择报告来源：扫描引擎或本平台。

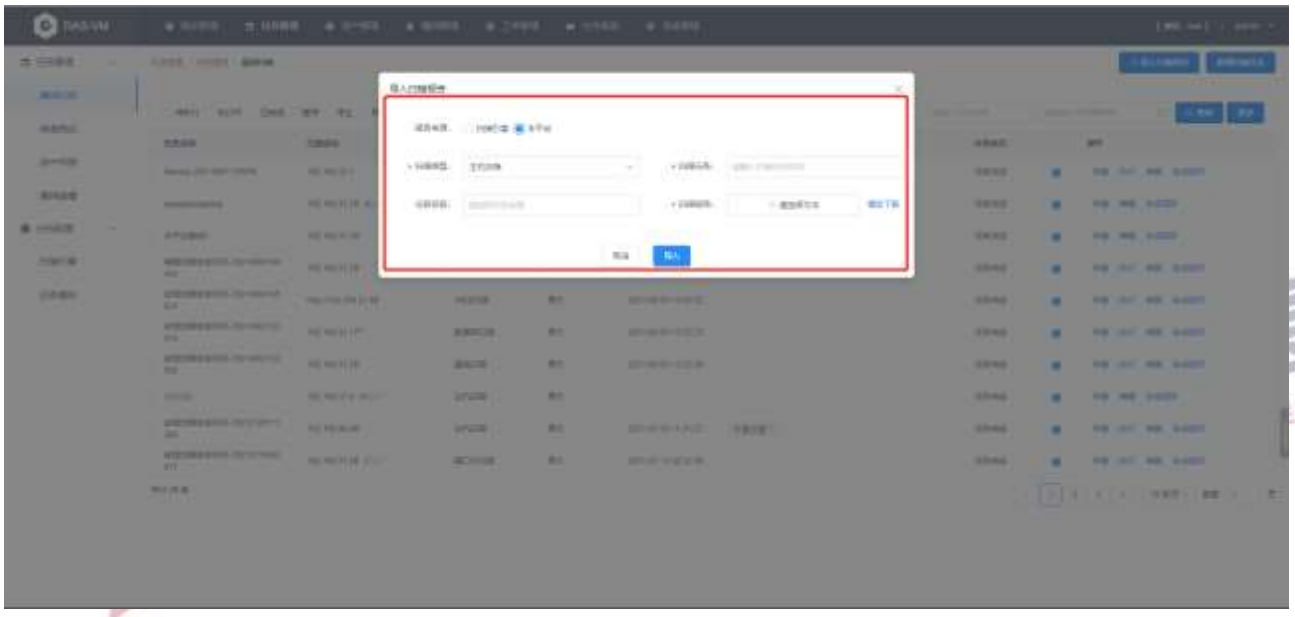
- 报告来源选择扫描引擎后，需要选择导入扫描报告的扫描引擎类型、扫描类型和扫描标签，输入扫描任务名称，点击<选择文件>按钮，选择要导入的扫描报告。



扫描引擎报告来源各类型扫描引擎支持的扫描类型及报告格式说明见下表：

扫描引擎	扫描类型	报告格式
安恒远程安全评估系统	主机扫描、web 扫描、基线扫描、弱口令扫描、数据库扫描	XML
绿盟远程安全评估系统	主机扫描、基线扫描、弱口令扫描	XML
Nessus	主机扫描	CSV
青藤云	主机扫描	HTML

- 报告来源选择本平台后，需要选择导入扫描报告的扫描类型和扫描标签，输入扫描任务名称，点击<选择文件>按钮，选择要导入的扫描报告。本平台来源的扫描报告仅支持 excel 格式，选择扫描类型后，单击<模板>可下载对应扫描类型的 excel 模板文件。



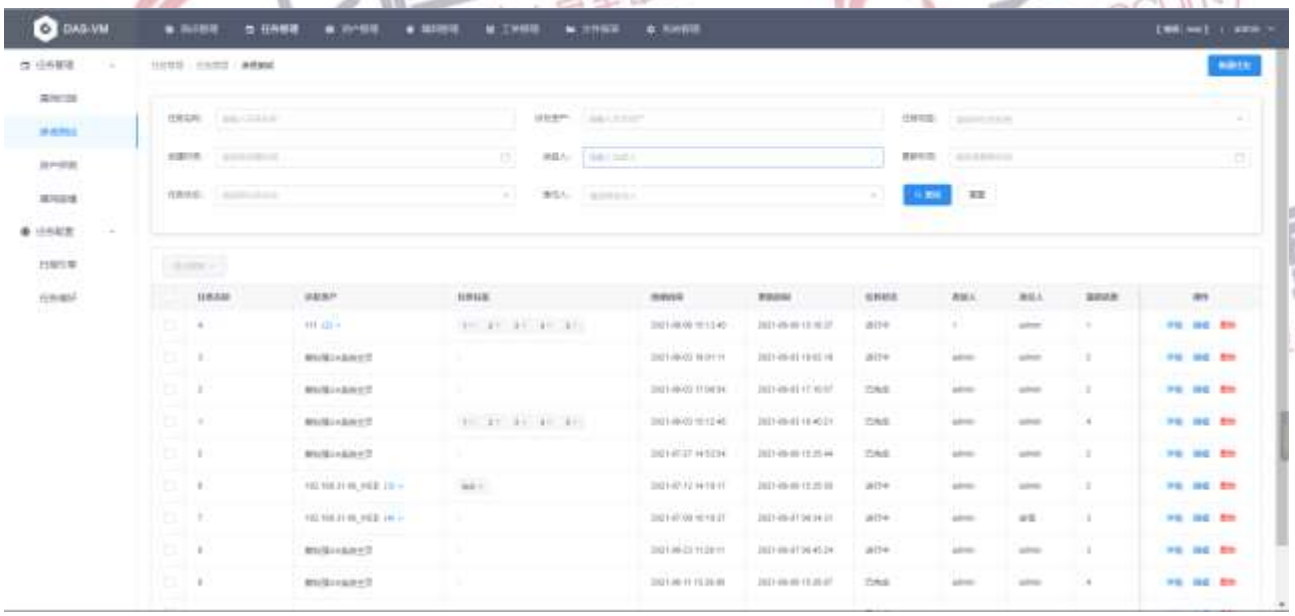
（3）点击<导入>按钮，会导入相应的扫描报告，可在扫描任务列表查看。

4.1.2. 渗透测试

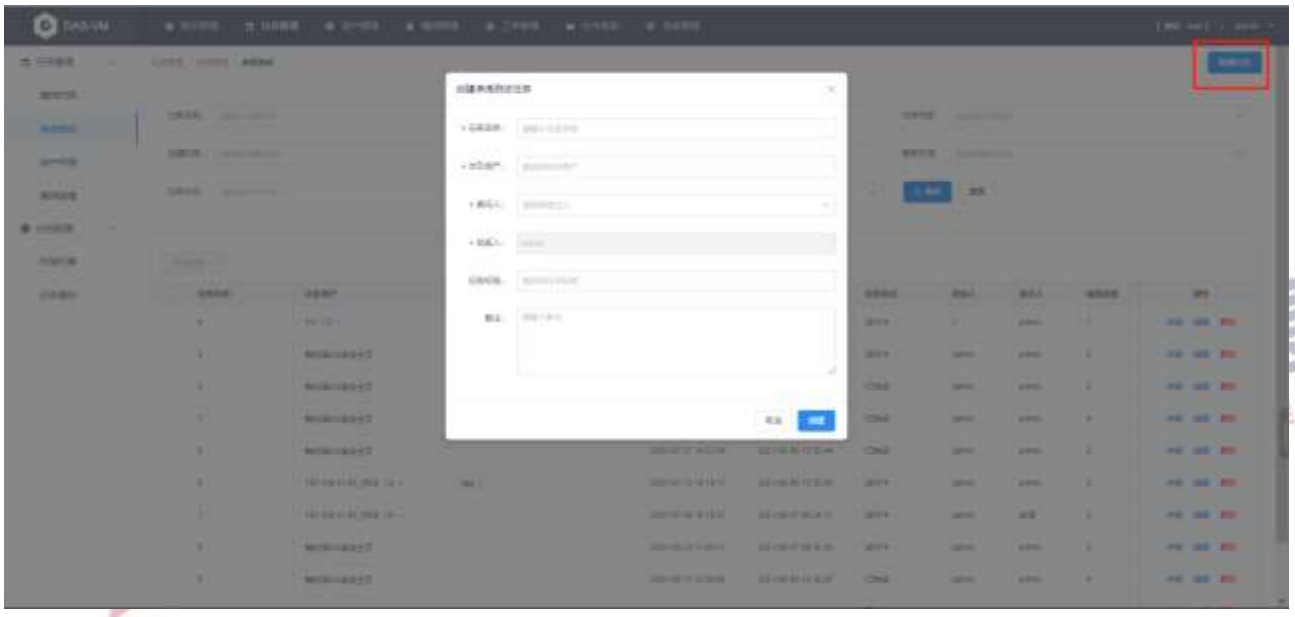
渗透测试功能用于记录未在扫描引擎中扫描出现的漏洞，通过人工录入的方式保存在平台。

4.1.2.1. 渗透任务新增

（1）用户 WEB 登录后，进入[任务管理 /任务管理 /渗透测试]页面。



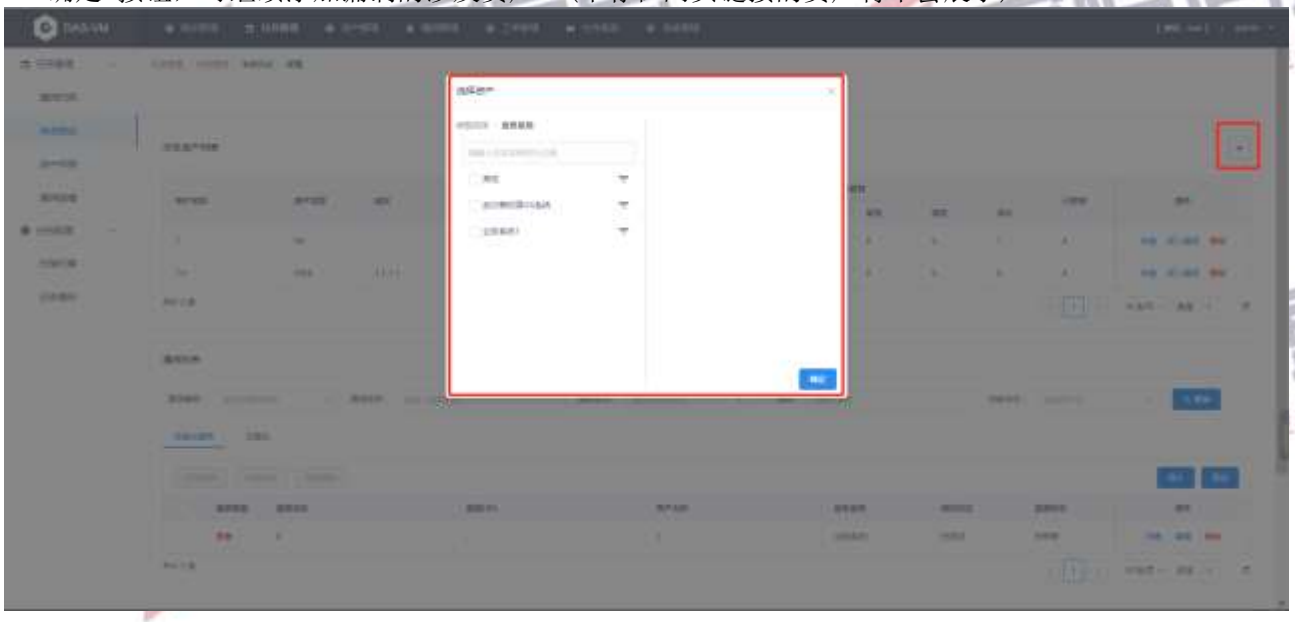
（2）点击右上角的<新建任务>按钮，弹出创建渗透测试任务弹窗，填写任务的基本信息，带有“*”符号的为必填项。点击<创建>按钮，进入任务详情页面，创建渗透测试任务时选中的涉及资产将添加到涉及资产列表中。



4.1.2.2. 涉及资产列表

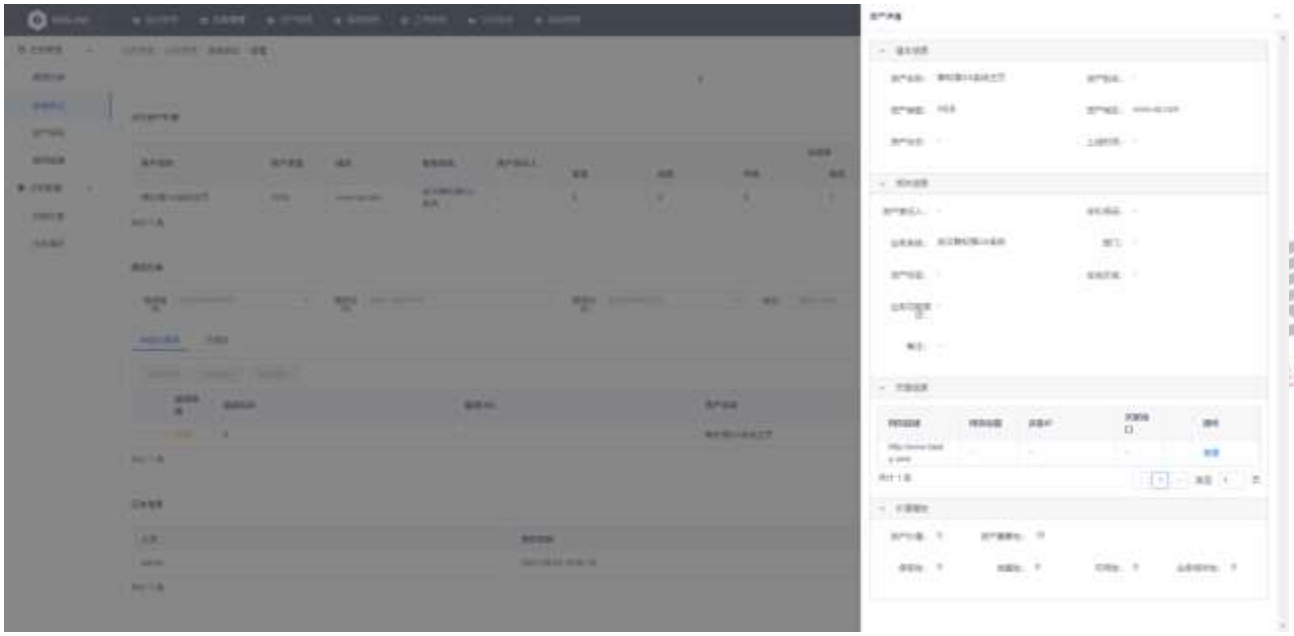
（1）涉及资产增加

点击渗透测试任务详情页涉及资产列表右上方的“+”符号，弹出资产选择窗，选择资产，点击〈确定〉按钮，可继续添加漏洞的涉及资产。（不存在网页链接的资产将不会展示）



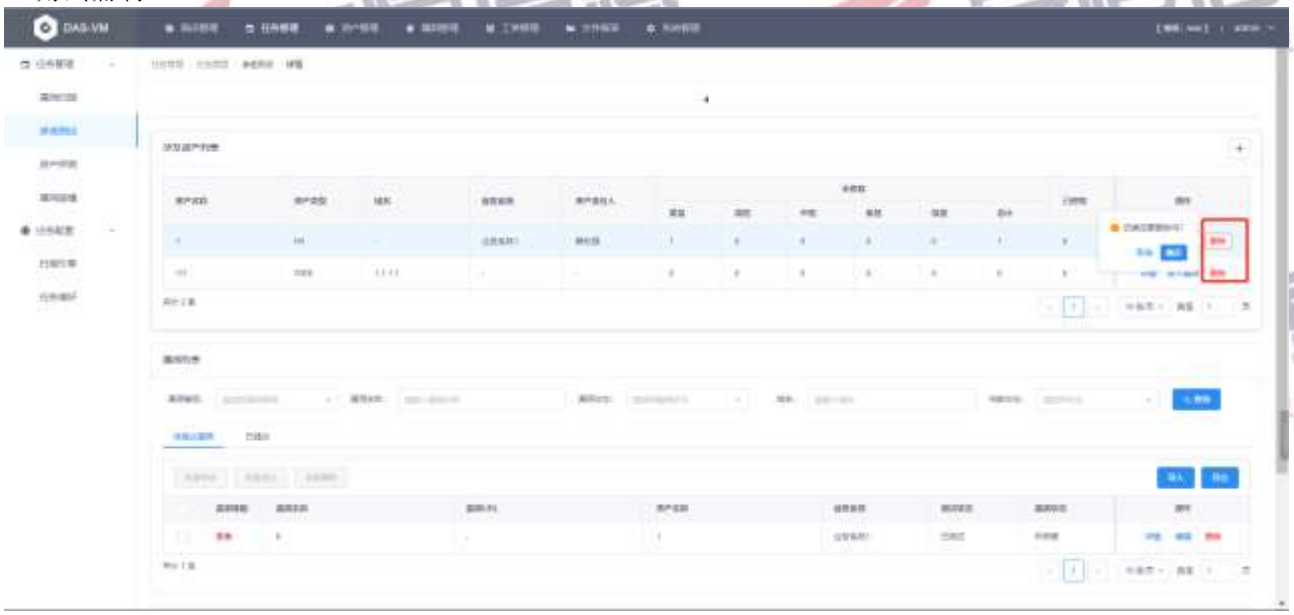
（2）涉及资产详情

点击涉及资产列表的〈详情〉按钮，弹出应用资产详情窗口，可查看相应的应用资产详细信息。



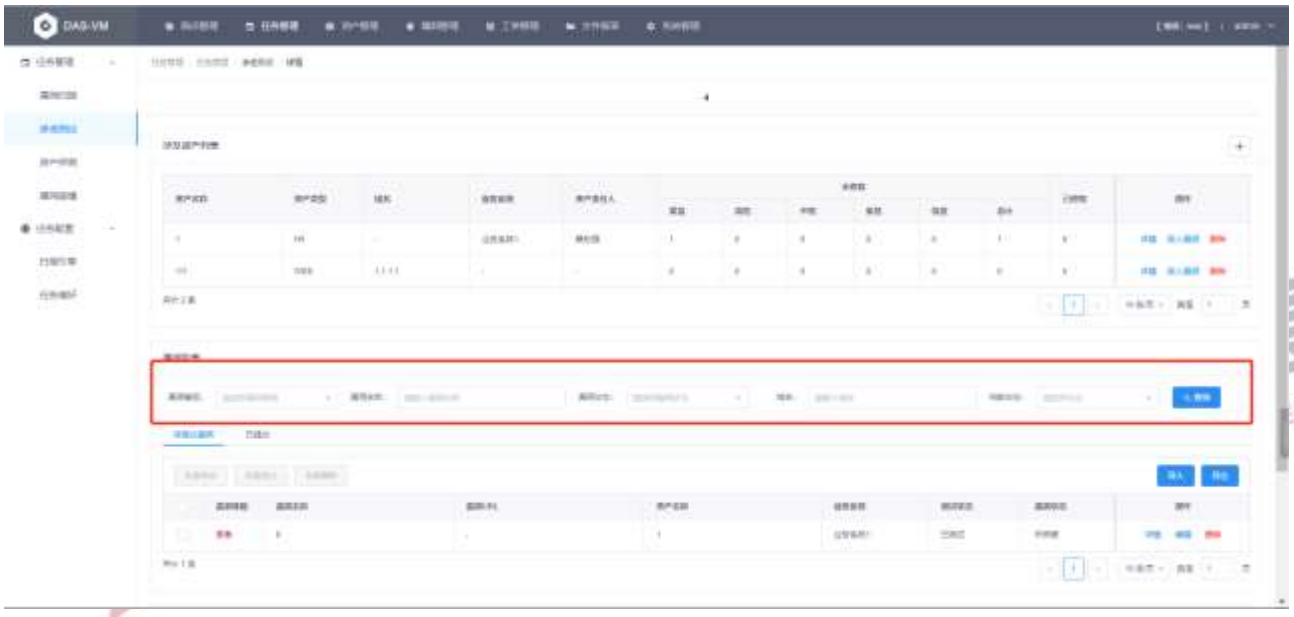
（3）涉及资产删除

点击涉及资产列表的<删除>按钮并确定，即可删除相应的涉及资产和该涉及资产下的所有渗透测试漏洞。



4. 1. 2. 3. 漏洞查询

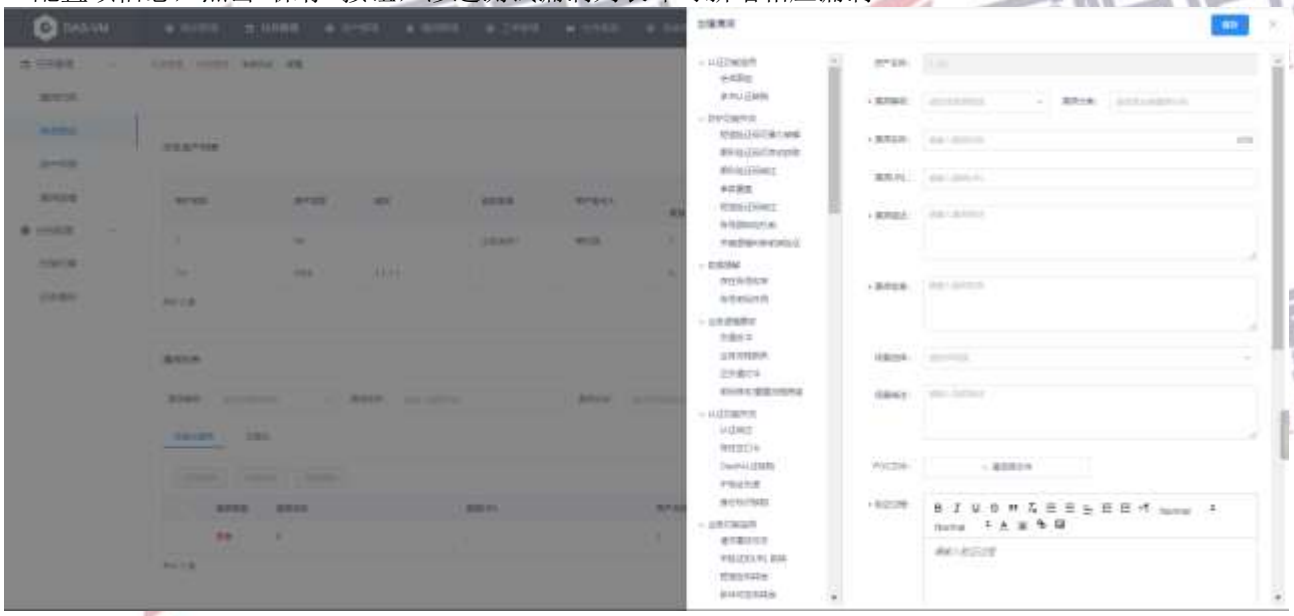
（1） 设置查询条件，可进行指定漏洞查询，条件设置后，点击<查询>按钮，进行查询。



4.1.2.4. 待提交漏洞列表

（1）漏洞录入

点击涉及资产列表中的<录入漏洞>按钮，弹出对应资产的创建漏洞窗口。填写渗透测试漏洞各配置项信息，点击<保存>按钮，渗透测试漏洞列表即可新增相应漏洞。



渗透测试漏洞各配置项相关说明见下表：

配置项	说明
资产名称	必填项，置灰。默认选中涉及资产的资产名称。
漏洞等级	必填项。包括信息、低危、中危、高危、紧急五个等级。
漏洞分类	选填项。录入漏洞的类型，可以选择左边分类。
漏洞名称	必填项。漏洞的名称。

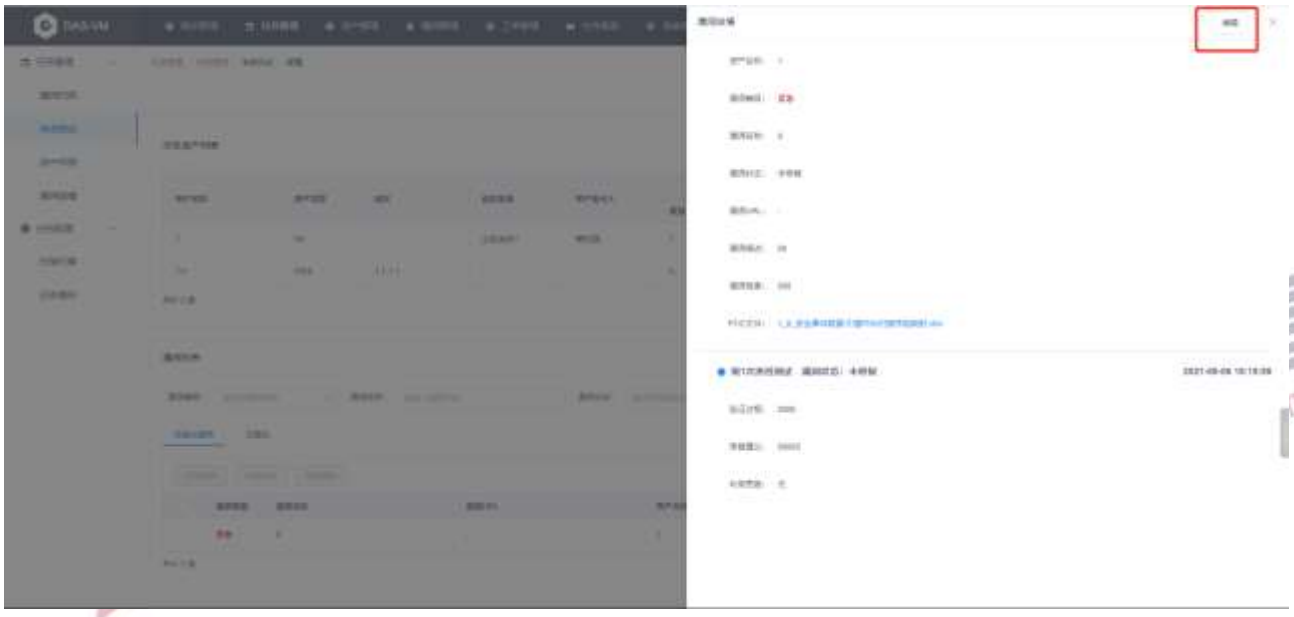
漏洞 URL	漏洞的位置链接，格式为 http(s)://开头的。
漏洞描述	必填项。选择左边分类后，自动填补，也可以手工输入进行补充。
漏洞危害	必填项。漏洞的危害。
场景选择	选填项。选择左边分类后，下拉会出现场景选择选项，选择漏洞所处的场景。
场景描述	选填项。漏洞出现的场景描述。
POC 文件	选填项。可上传 POC 文件。
验证过程	必填项。填写验证漏洞的过程，支持图片、文本形式。
修复建议	必填项。填写漏洞的修复建议方案，支持图片、文本形式。
利用思路	选填项。填写利用此漏洞的思路，支持图片、文本形式。

（2）漏洞详情

点击漏洞列表中的<详情>按钮，弹出漏洞详情窗口，可查看相应漏洞的详细信息。

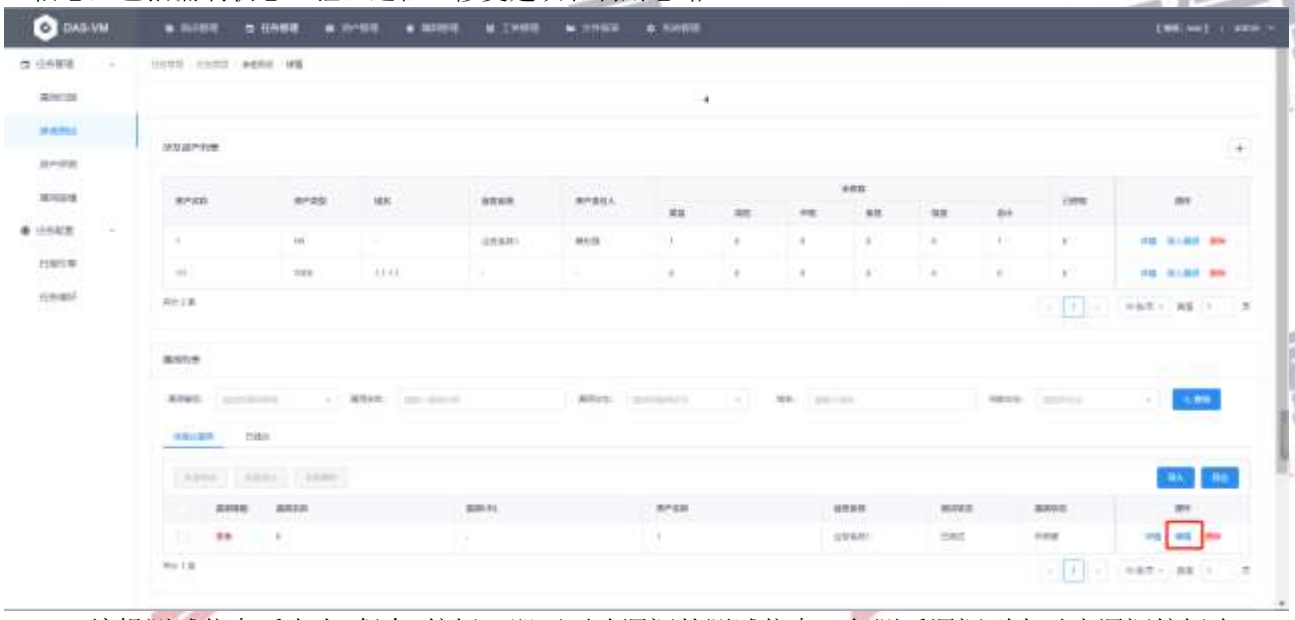
（3）漏洞详情编辑

点击漏洞详情窗口的<编辑>按钮，弹出漏洞基本信息编辑窗口，可编辑漏洞的基本信息，包括漏洞等级、漏洞分类、漏洞名称、问题链接、漏洞描述 、漏洞危害、场景选择、场景描述和 POC 文件。编辑基本信息后点击<保存>按钮，即可更改漏洞的基本信息，点击<取消>按钮，即可取消更改漏洞的基本信息。

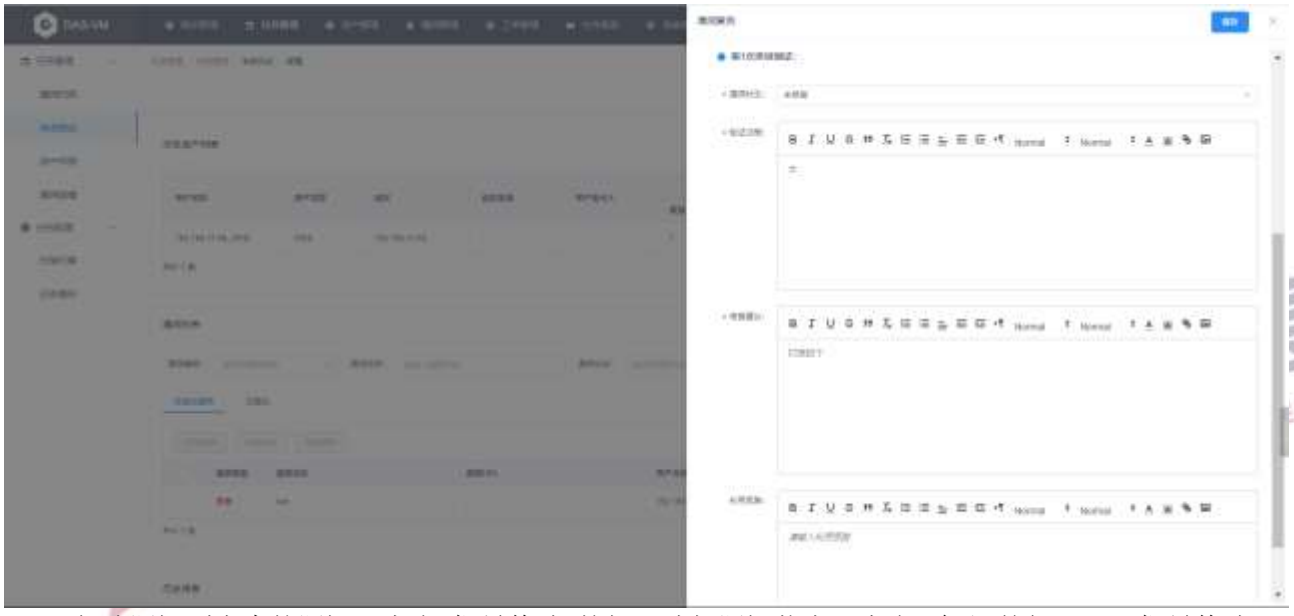


（4）漏洞复测/编辑

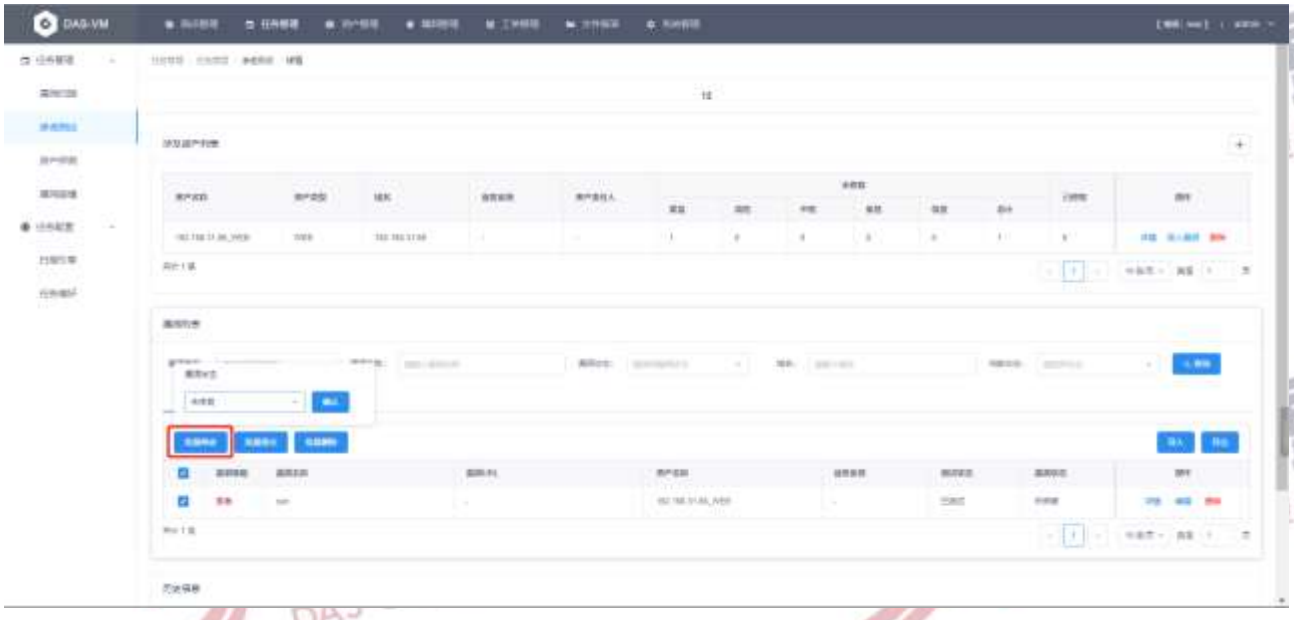
点击待提交漏洞列表中的<复测>或<编辑>按钮，弹出漏洞测试信息编辑窗口，可编辑漏洞测试信息，包括漏洞状态、验证过程、修复建议和利用思路。



编辑测试信息后点击<保存>按钮，即可更改漏洞的测试信息。复测后漏洞列表对应漏洞按钮由<复测>变更为<编辑>。

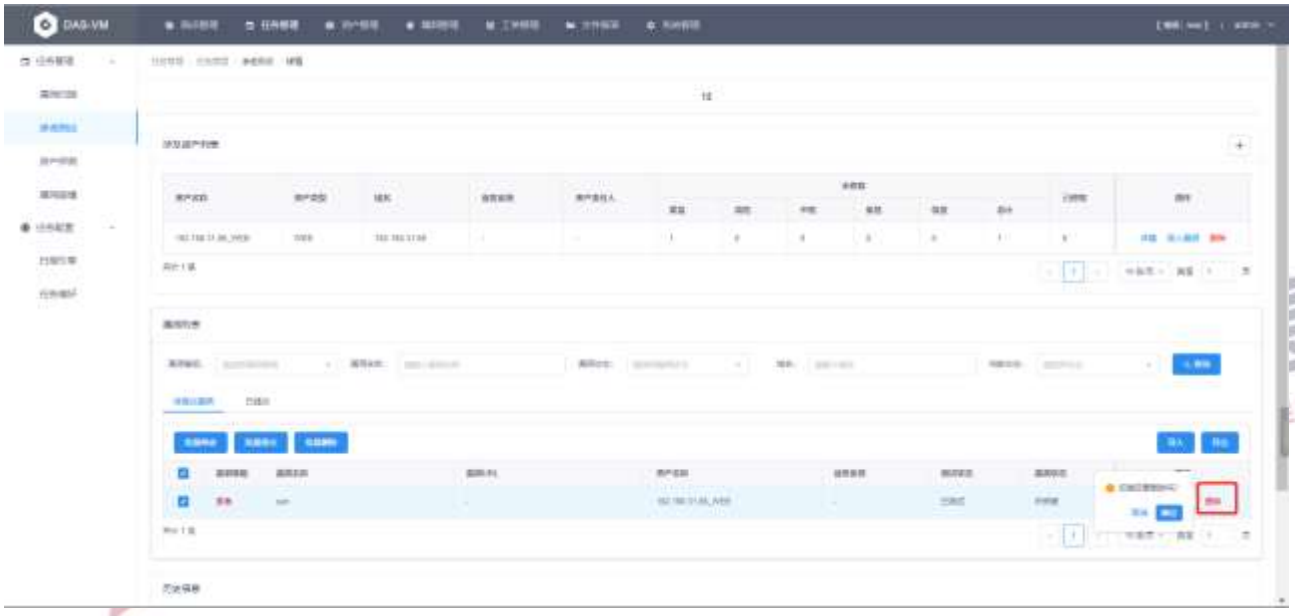


勾选漏洞列表中的漏洞，点击<批量修改>按钮，选择漏洞状态，点击<确认>按钮，即可批量修改所有勾选漏洞的本次测试漏洞状态



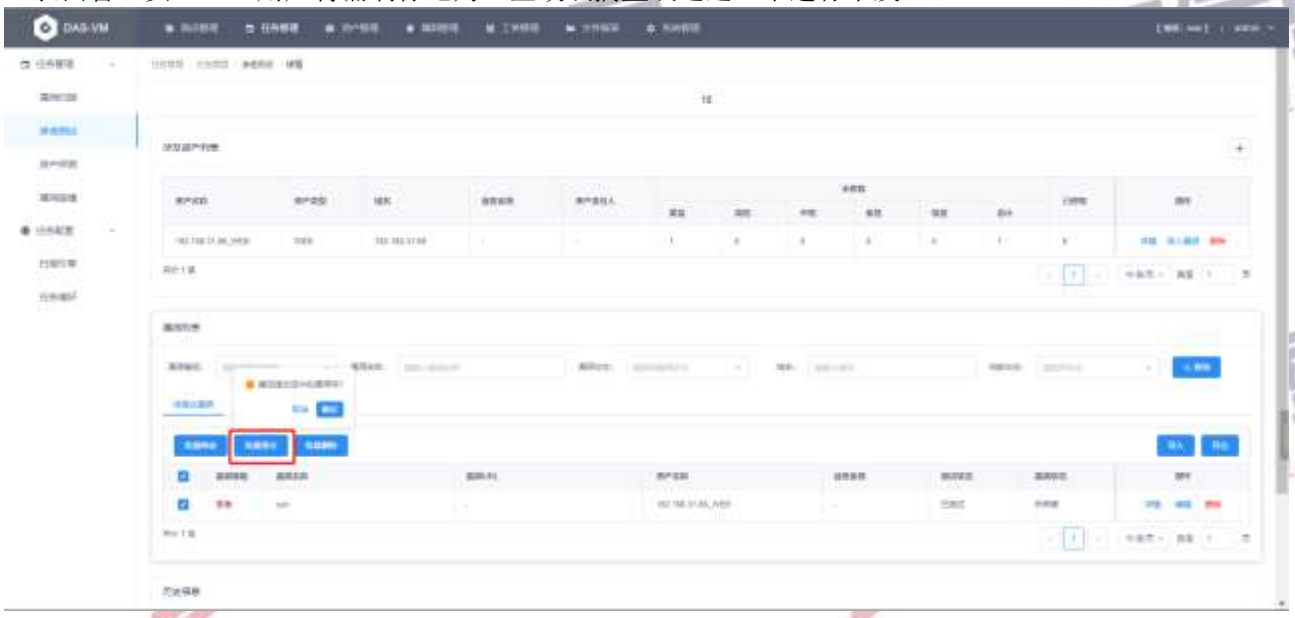
（5）漏洞删除

点击漏洞列表的<删除>按钮并确定，即可删除对应漏洞。



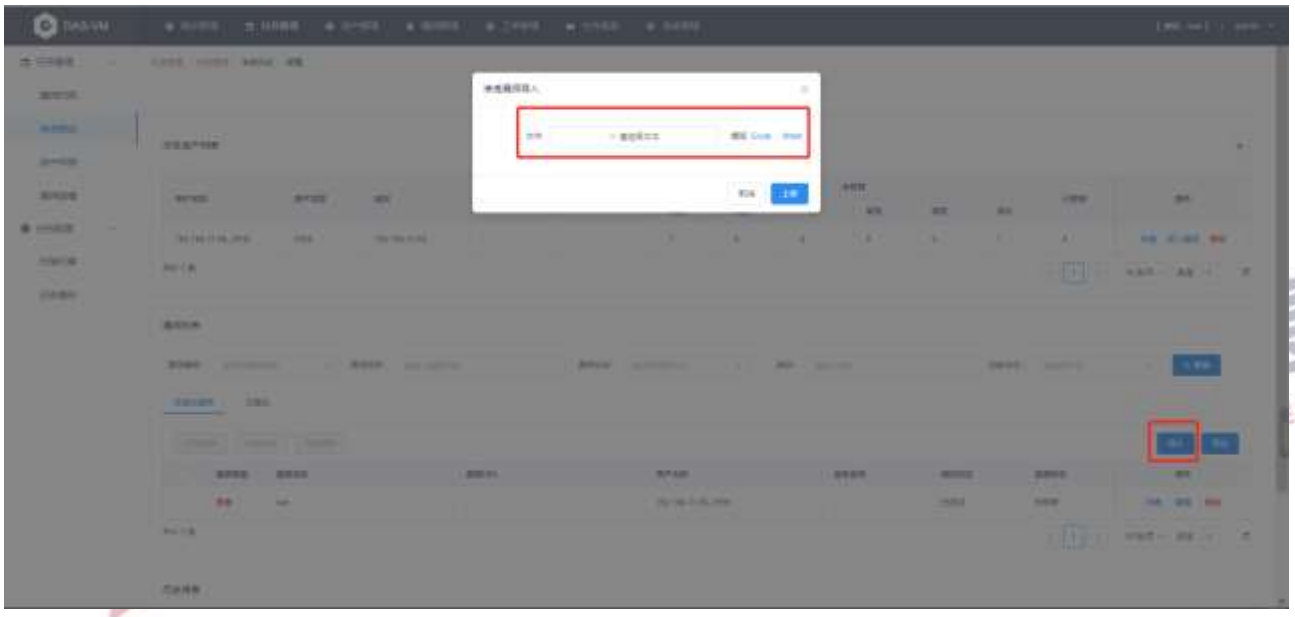
（6）漏洞提交

勾选漏洞点击<批量提交>按钮可提交漏洞至已提交漏洞列表，未修复的漏洞可在已提交漏洞列表由管理员 admin 用户将漏洞标记为已整改或搁置或通过工单进行下发。



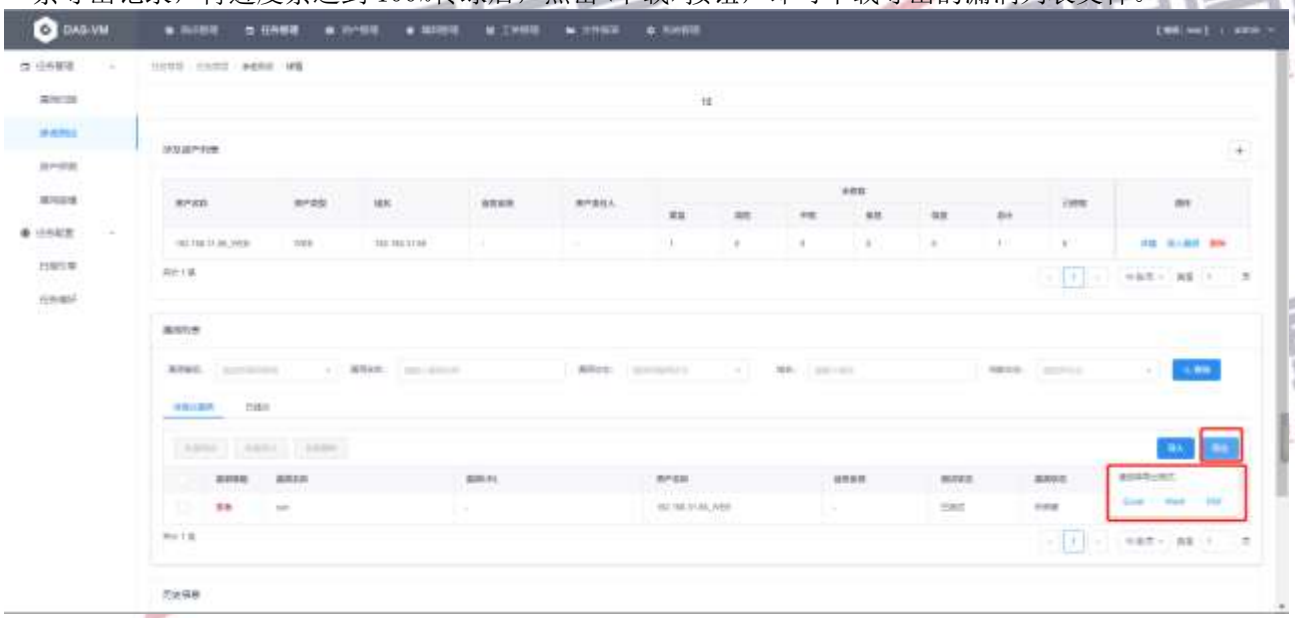
（7）漏洞导入

点击待提交漏洞列表右上方的<导入>按钮，选择相应的 word 或 excel 文件后，点击<上传>按钮可以批量导入漏洞，也可以下载模板文件，编辑后再导入。



（8）漏洞导出

点击待提交漏洞列表右上方的<导出>按钮，选择格式（包括 excel、word 和 pdf），可以导出所有漏洞，页面跳转至[文件报表/报表管理 /下载管理]页面，[文件报表/报表管理 /下载管理]页面新增一条导出记录，待进度条达到 100%转绿后，点击<下载>按钮，即可下载导出的漏洞列表文件。

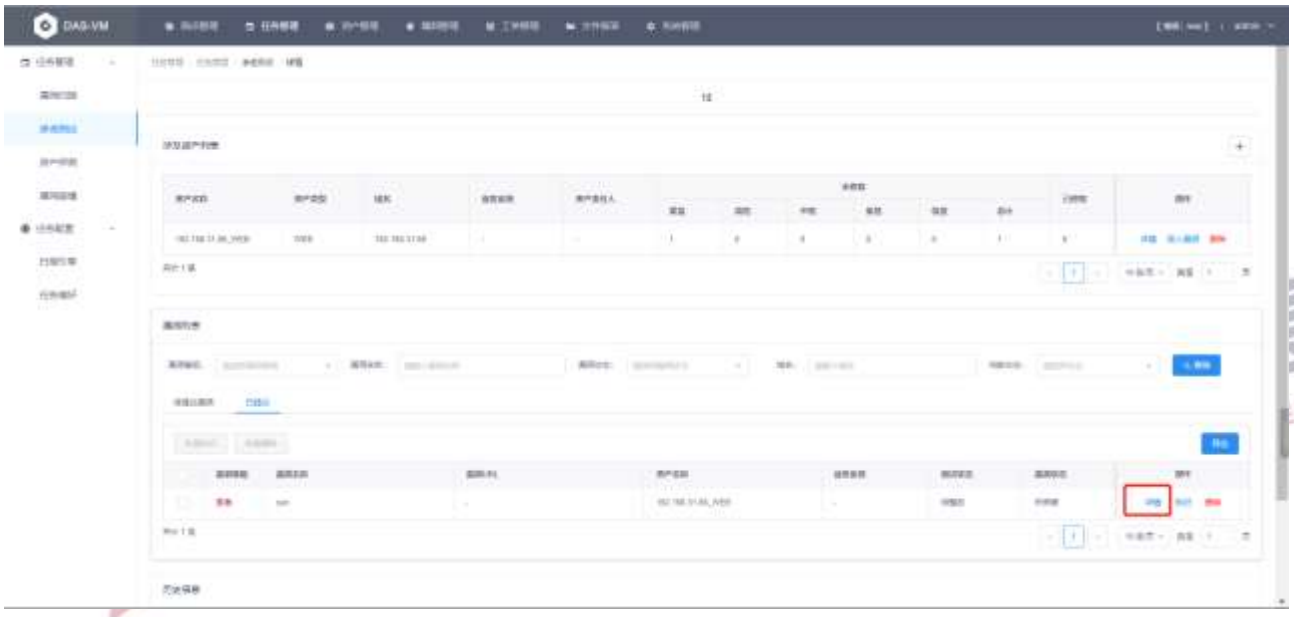


4.1.2.5. 已提交漏洞列表

漏洞进入已提交列表后，若不进行工单下发，仅管理员 admin 用户存在权限可以将漏洞标记为已整改或搁置、对漏洞详情进行编辑、删除漏洞等操作；仅已经进行提交后的漏洞才可以在工单操作中进行下发。

（1）漏洞详情

点击已提交漏洞列表中的<详情>按钮，弹出漏洞详情窗口，可查看相应漏洞的详细信息。

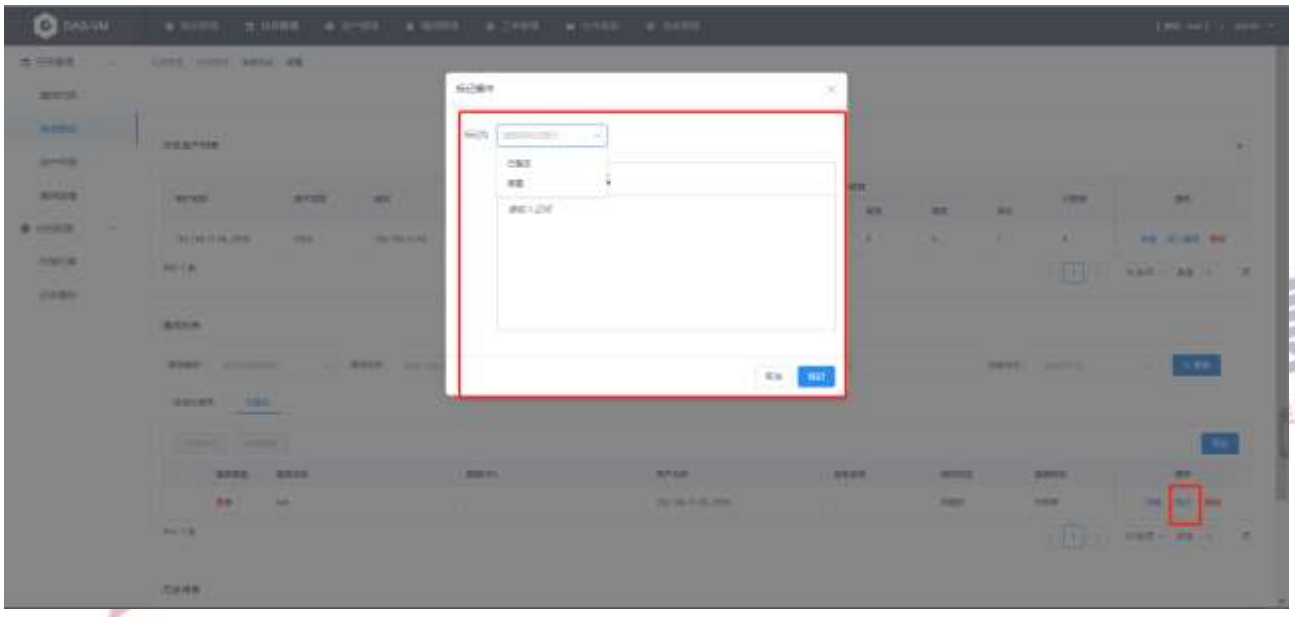


（2）漏洞详情编辑

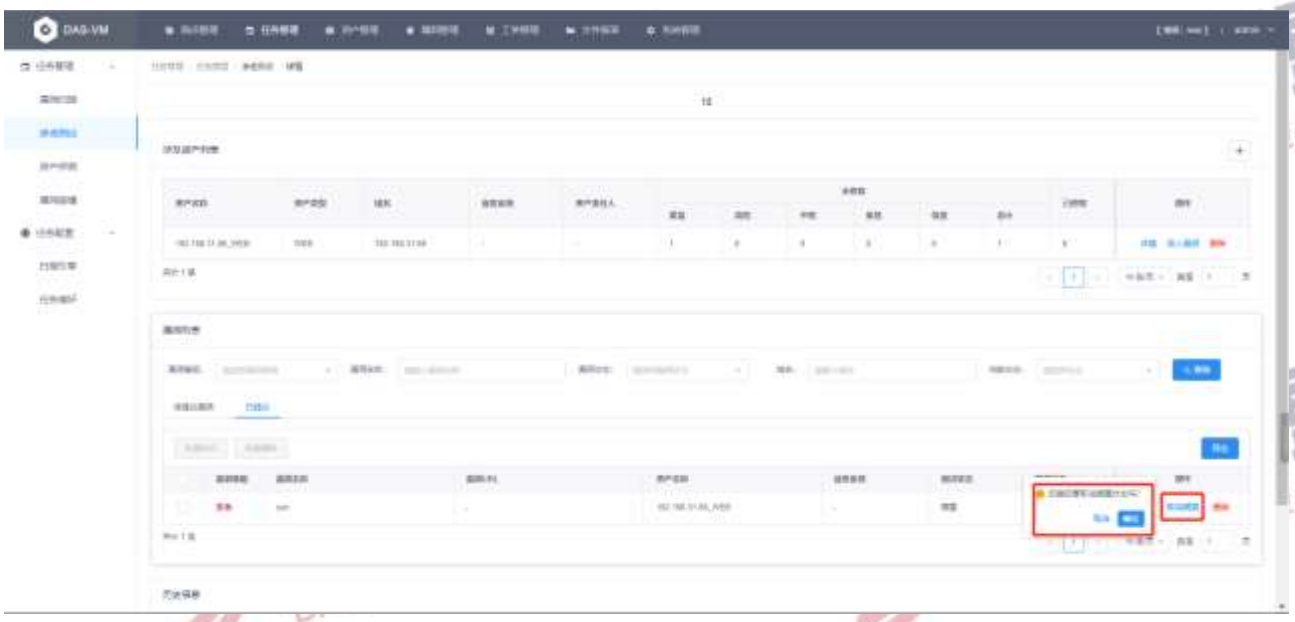
点击漏洞详情窗口的<编辑>按钮，弹出漏洞基本信息编辑窗口，可编辑漏洞的基本信息，包括漏洞等级、漏洞分类、漏洞名称、问题链接、漏洞描述 、漏洞危害、场景选择、场景描述和 POC 文件。编辑基本信息后点击<保存>按钮，即可更改漏洞的基本信息，点击<取消>按钮，即可取消更改漏洞的基本信息。

（3）漏洞整改

点击已提交漏洞列表中的<标记>按钮或勾选漏洞点击<批量标记>按钮，选择标记状态，填写证明，点击<标记>按钮。

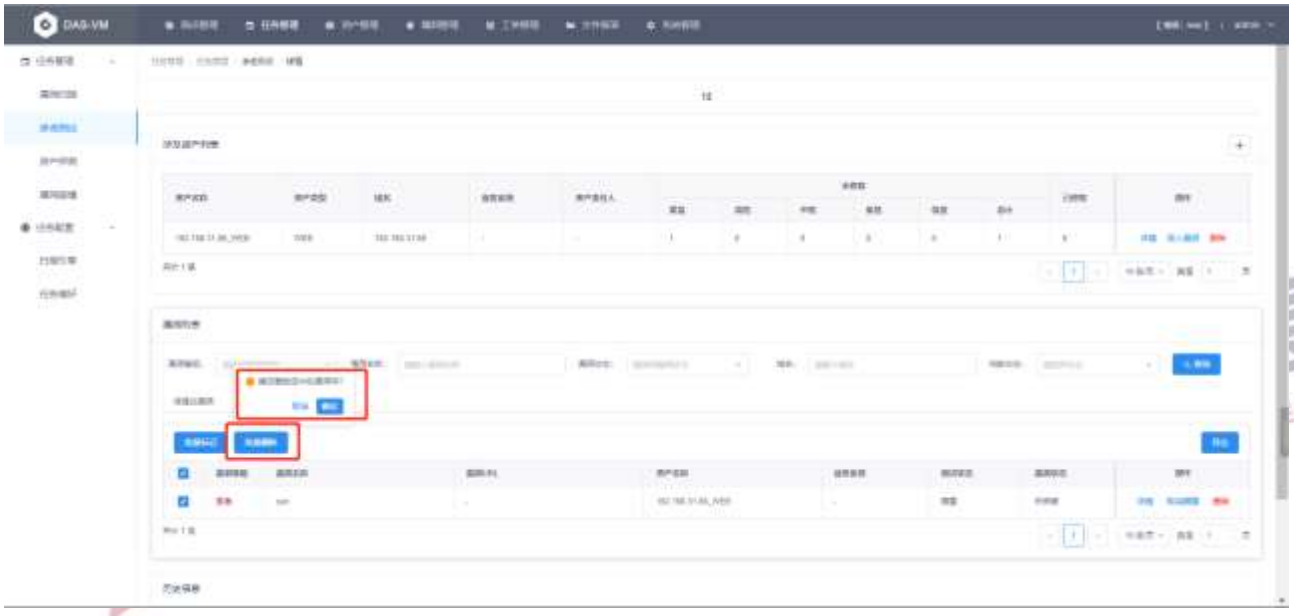


- 标记为已整改的漏洞将自动提交到待提交漏洞列表进行复测。
- 标记为搁置的漏洞将继续留在已提交漏洞列表，可点击<取消搁置>按钮取消搁置后重新标记。



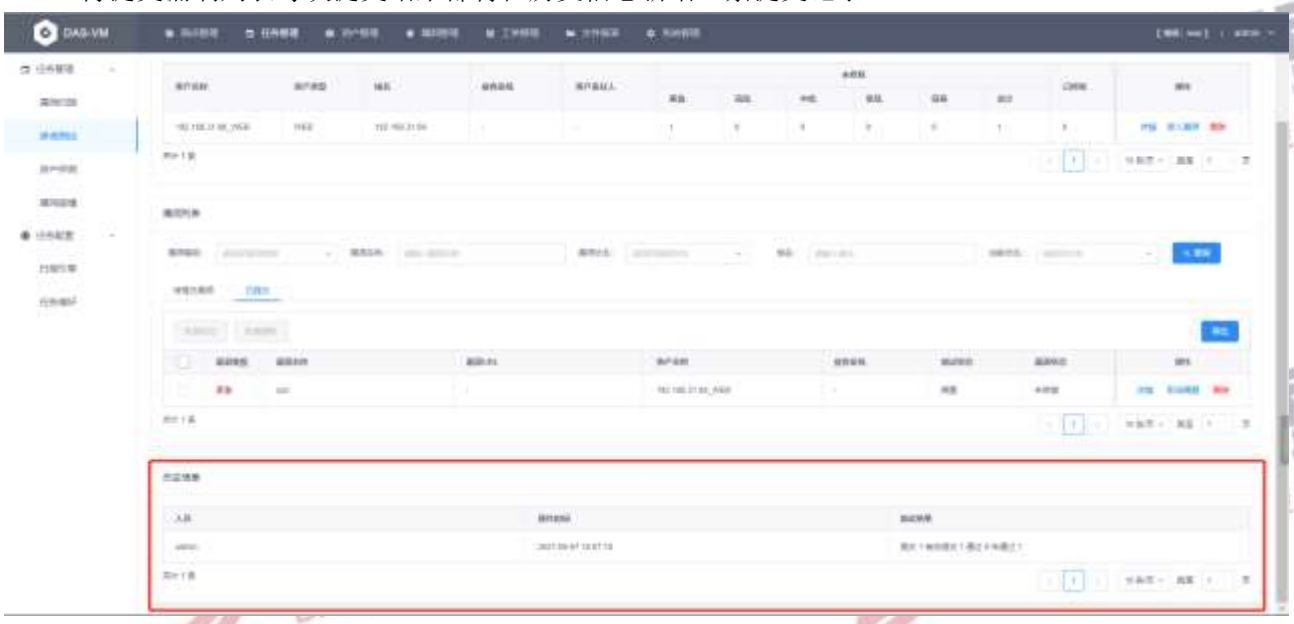
（4）漏洞删除

点击漏洞列表的<删除>按钮并确定或勾选漏洞点击<批量删除>按钮并确定，即可删除对应漏洞。



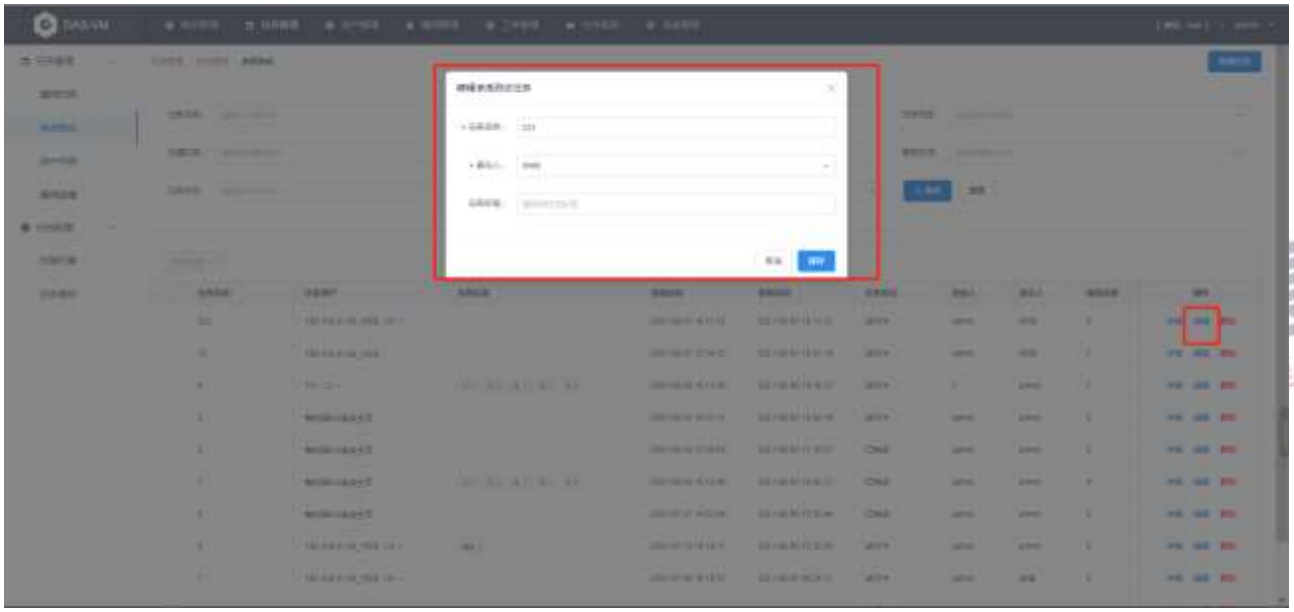
4.1.2.6. 历史信息

（1） 待提交漏洞列表每次提交结果都将在历史信息新增一条提交记录。



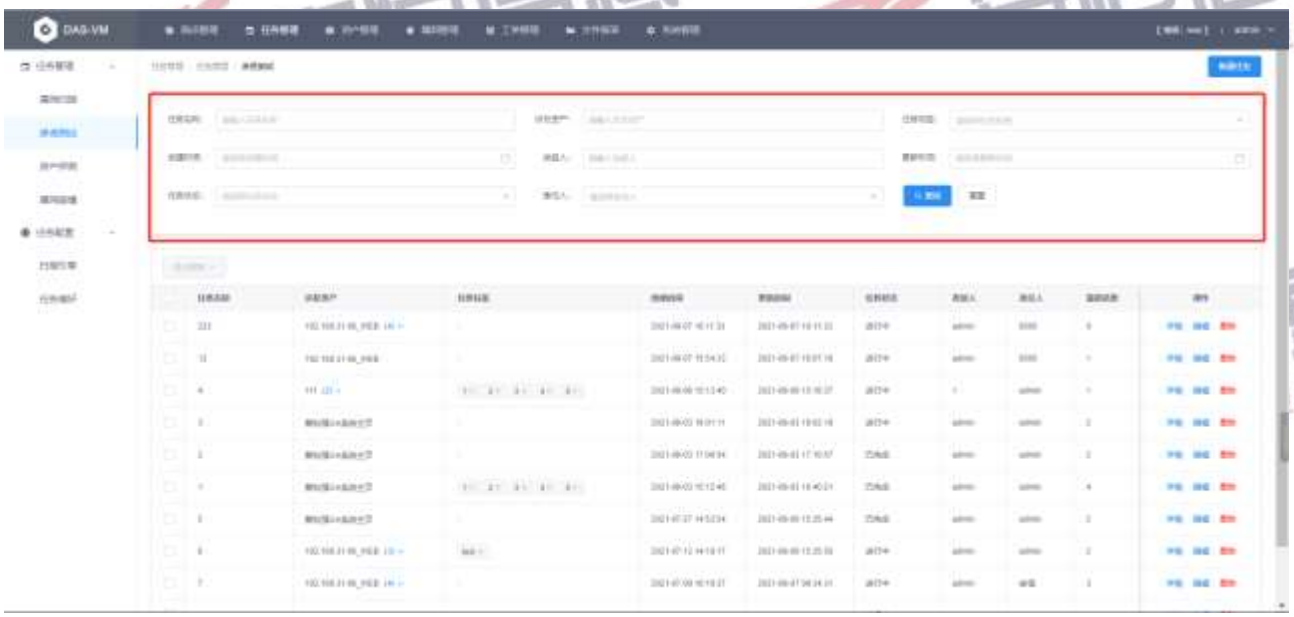
4.1.2.7. 渗透测试任务编辑

（1） 点击渗透测试任务列表中的<编辑>按钮，弹出编辑渗透测试任务窗口，编辑渗透测试任务信息，包括任务名称、责任人和任务标签，点击<保存>按钮，即可修改相应的渗透测试任务信息。



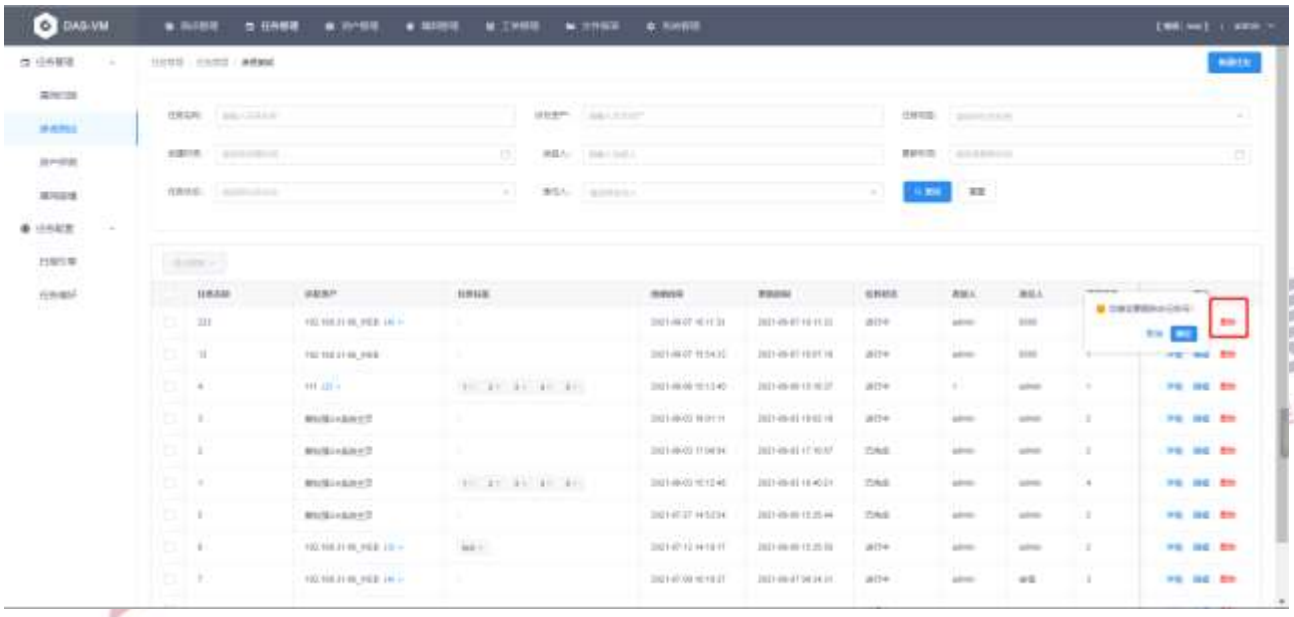
4.1.2.8. 渗透测试任务查询

（1） 设置查询条件，可进行指定渗透测试任务查询，条件设置后，点击<查询>按钮，进行查询。点击<重置>按钮，可清空查询条件。



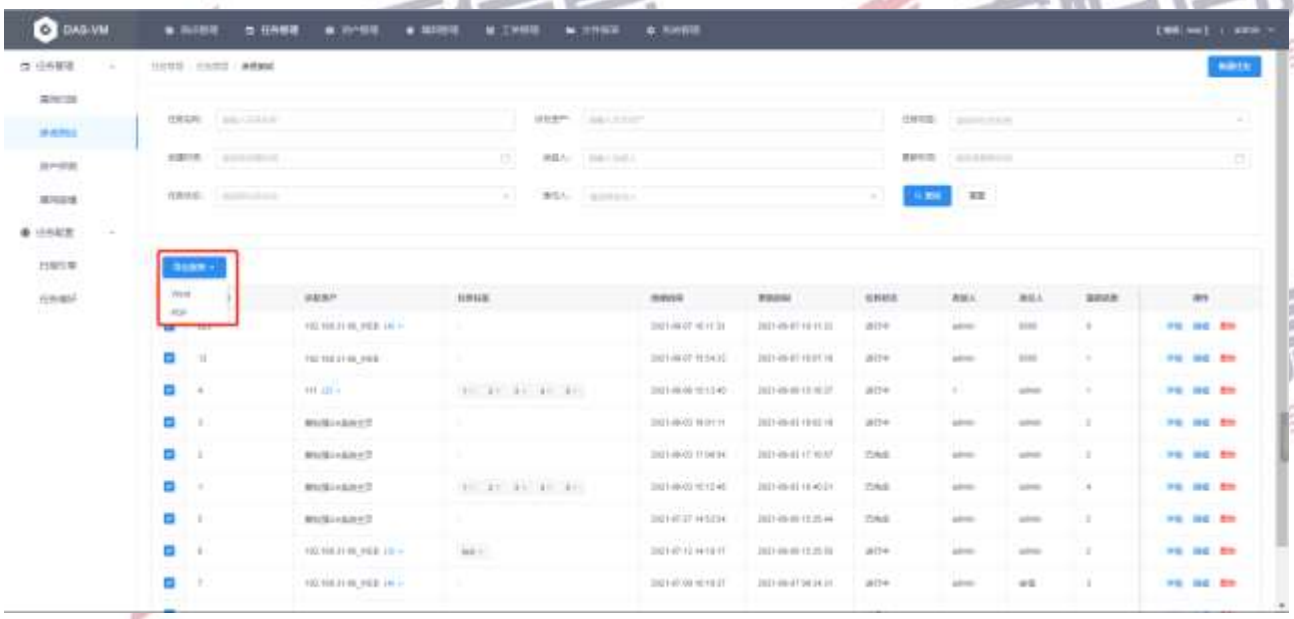
4.1.2.9. 渗透测试任务删除

（1） 点击渗透测试任务列表中的<删除>按钮并确定，即可删除对应渗透测试任务。

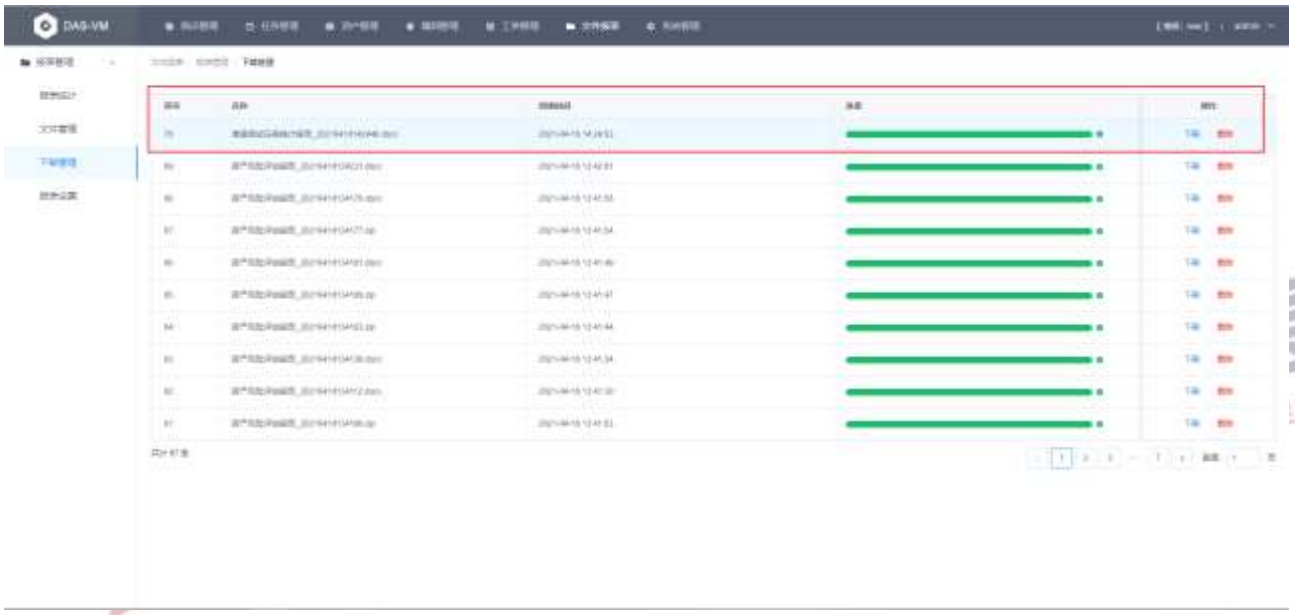


4.1.2.10. 渗透测试报表导出

（1）勾选渗透测试任务，点击<导出报表>按钮，下拉展开导出格式选项，选择导出格式 Word 或 PDF，可以导出选中渗透测试任务指定格式的统计报表，页面跳转至[文件报表/报表管理 /下载管理]页面。



（2）[文件报表/报表管理 /下载管理]页面新增一条导出记录，待进度条达到 100%转绿后，点击<下载>按钮，即可下载导出的渗透测试任务统计报告。



4.1.3. 资产探测

资产探测可以查看扫描引擎的资产探测任务下发与简单的任务结果，具体包括以下几个方面的内容：资产探测任务创建和执行、探测进度查看、探测结果查看。

4.1.3.1. 探测任务新增

（1） 用户 WEB 登录后，进入[任务管理 /任务管理 /资产探测]页面。

（2） 点击右上角的<新增探测任务>按钮。弹出新增探测任务窗口，默认进入基本信息页面，选择扫描工具、扫描类型和任务标签，输入任务名称和备注。

新增探测任务基本信息配置项及说明见下表：

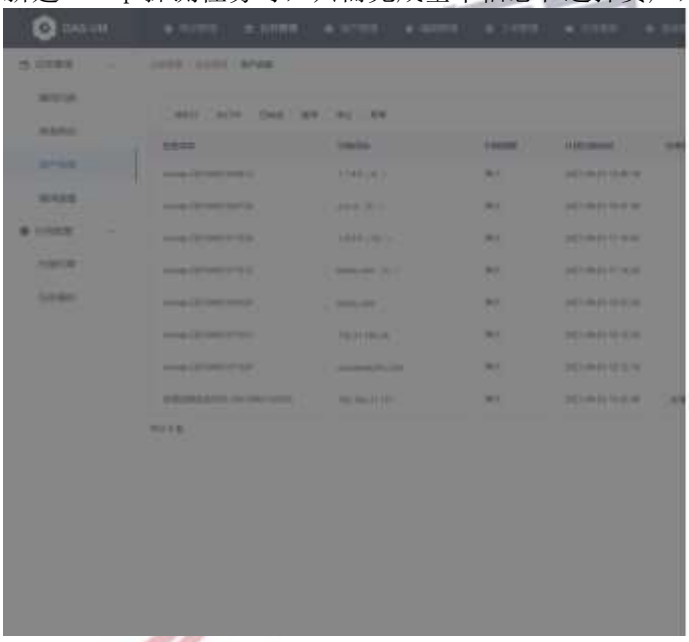
配置项	说明
扫描工具	必填项。选择扫描工具，可选扫描引擎管理列表中已添加成功的扫描引擎。
扫描类型	必填项，默认资产探测，置灰。
任务名称	必填项。新增探测任务的任务名称。
任务标签	选填项。选择任务标签，将探测任务归类到对应个标签下。
发起人	必填项，置灰。默认创建探测任务的发起人，即当前登录用户。
备注	选填项。新增探测任务的注解说明。

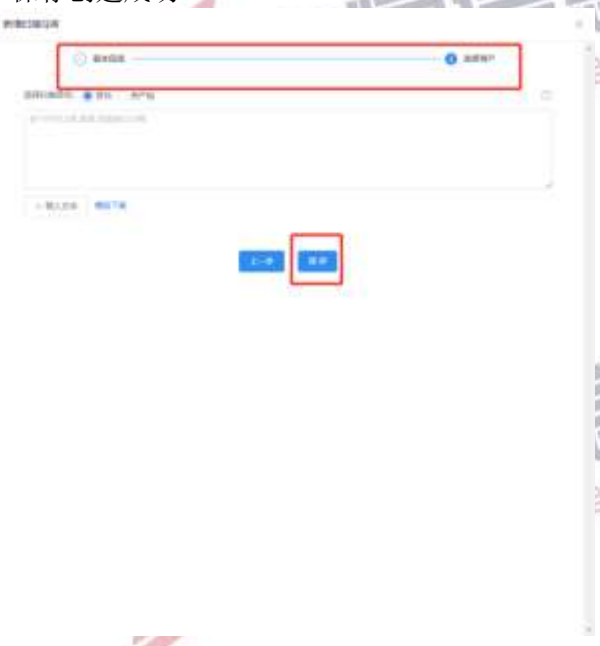
（3） 点击<下一步>按钮进入选择资产页面，输入扫描目标，可以输入 IP 地址或搜索资产组进行选择。

新增探测任务选择资产配置项及说明见下表：

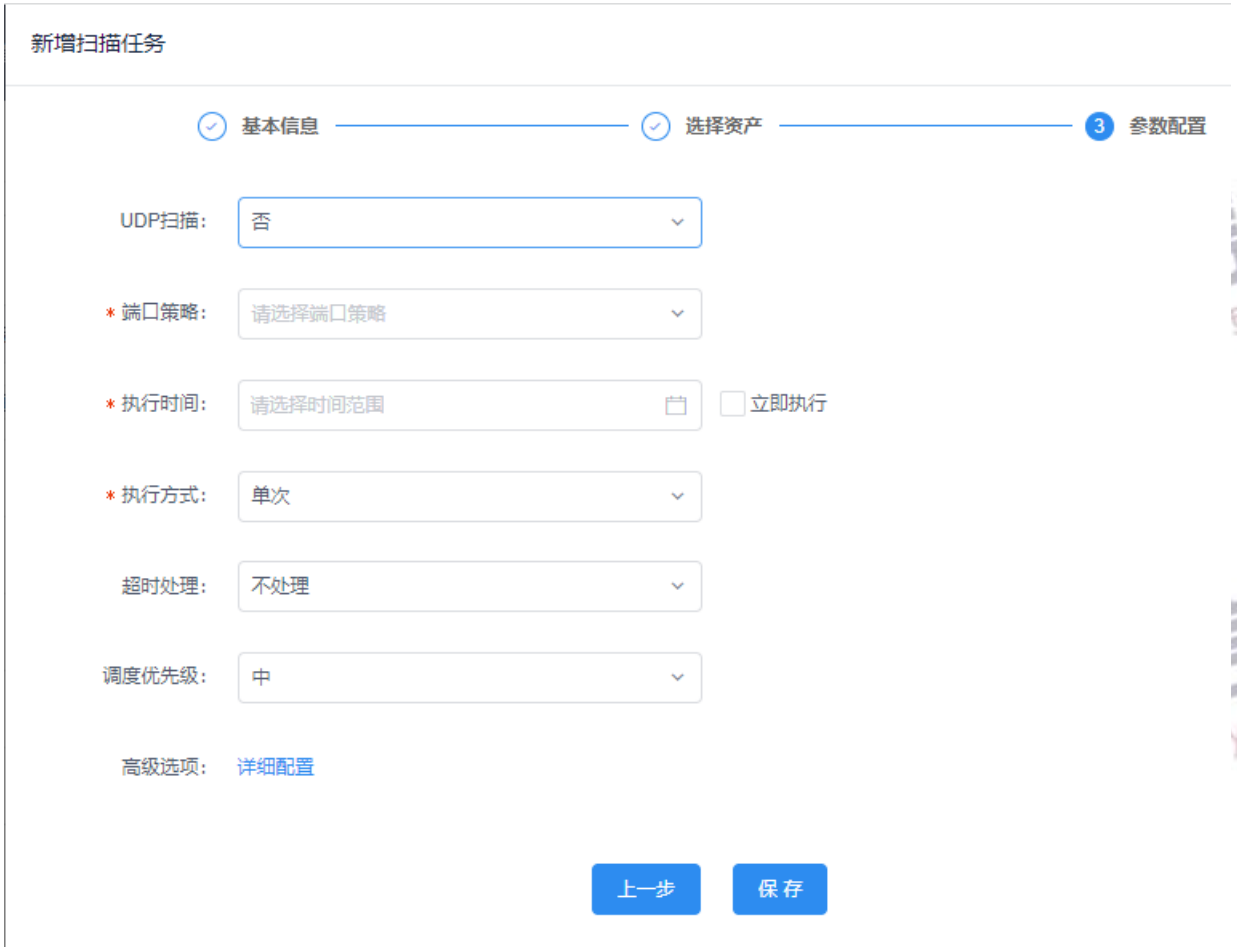
配置项	说明
IP 地址	可以添加单个 IP 地址或 IP 段，如：192.168.0.1 或 192.168.1.1-254
资产组	可以直接选择平台已添加的资产组或单个资产，可通过名称搜索具体资产
导入文件	可通过导入 excel 文件批量导入 IP 地址等扫描目标
?	提示图标，可以显示扫描目标格式示例

新建 sumap 探测任务时，只需完成基本信息和选择资产，保存创建成功。





（4）点击<下一步>按钮进入参数配置页面，选择端口策略、执行时间、是否立即执行、执行方式、超时处理、调度优先级等内容，点击<保存>按钮，探测任务创建完成。



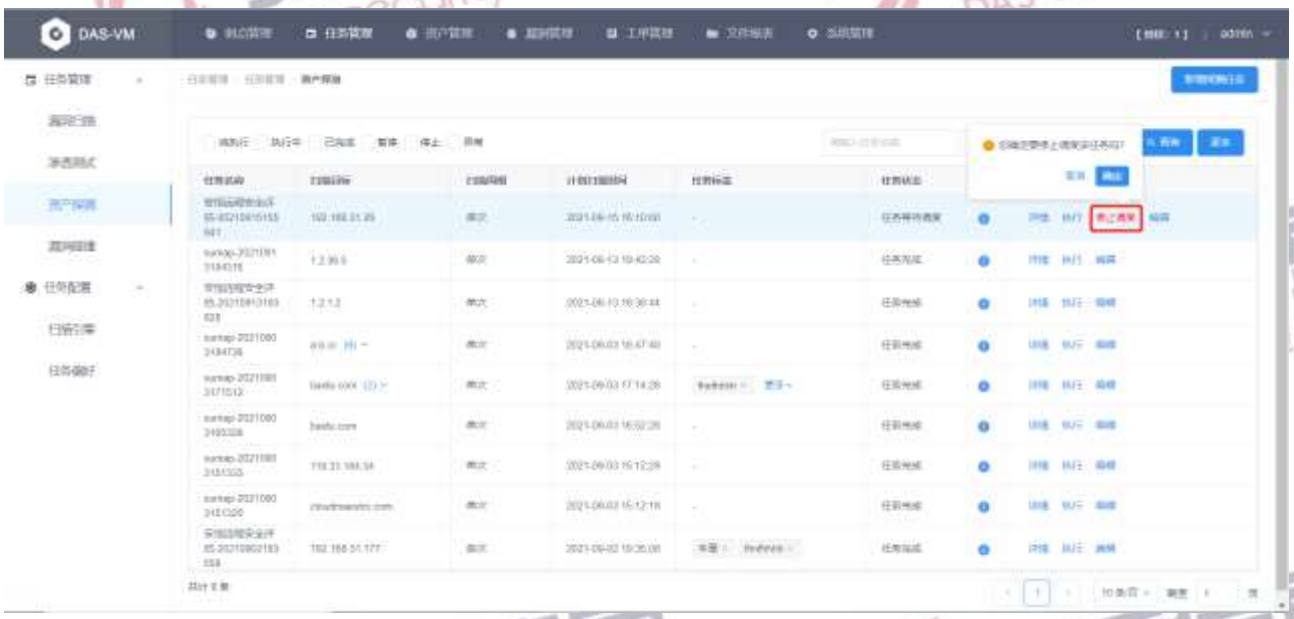
新增探测任务参数配置配置项及说明见下表：

配置项	说明
端口策略	必填项。发往扫描引擎的探测任务执行端口策略。
UDP 扫描	选填项。选择是否进行 UDP 扫描。
执行时间	必填项。扫描引擎正式开始扫描的时间。
立即执行	勾选项。扫描引擎执行是否立即执行一次。
执行方式	必填项。扫描引擎执行扫描的周期，可选择：单次、每天、每周、每月、每年，与执行时间组合搭配。
超时处理	选填项。扫描任务超时对扫描任务的处理方式，可选项有：不处理、暂停、停止。
超时时间	选填项。超时处理方式选择暂停或停止时，此选项才会被激活，可选择超时时间：10 小时、5 小时、2 小时。

调度优先级	选填项。扫描任务优先级，可选：高、中、低。
高级选项	选填项。资产探测高级配置，仅用于安恒远程安全评估。
扫描深度	选填项。可选择深度：1、2、3、4、5，值越大，插件获取的信息可能就越多，相应的扫描时间会更长，仅用于绿盟远程安全评估。
插件超时限制	选填项。范围：1-300，单位：秒，单个插件在指定时间内如果未正常结束将会被调入引擎终止，仅用于绿盟远程安全评估。

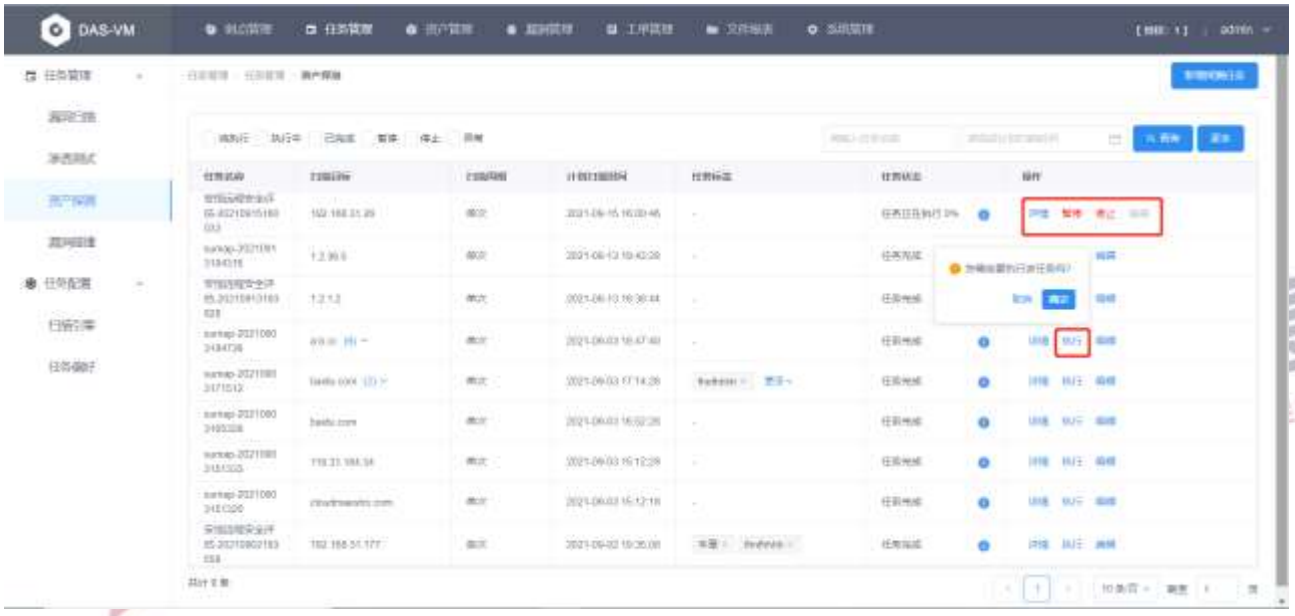
4.1.3.2. 探测任务停止调度

（1） 当任务处于等待调度状态时，点击任务列表的<停止调度>按钮并确定，可停止调度扫描任务。



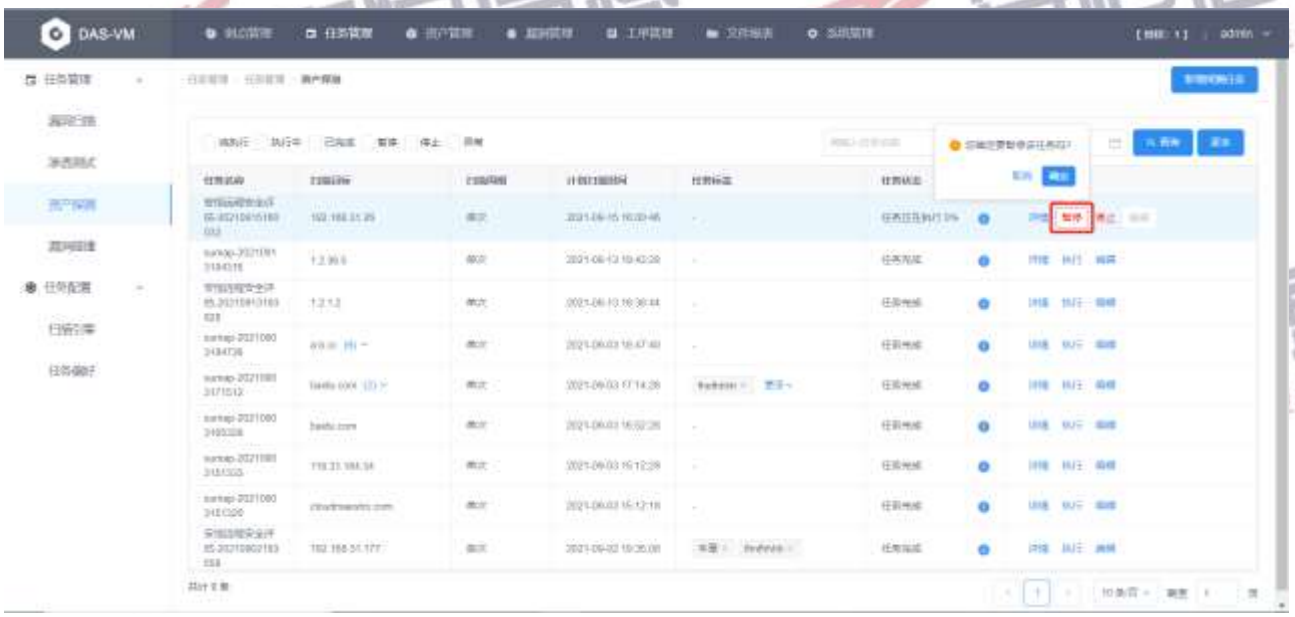
4.1.3.3. 探测任务执行

（1） 点击任务列表的<执行>按钮并确定，可立即执行一次对应的探测任务。任务开始执行后，右侧操作栏按钮变为<详情>、<暂停>、<停止>和<编辑>，可以查看任务详情或对任务进行暂停、停止等操作，<编辑>按钮置灰。

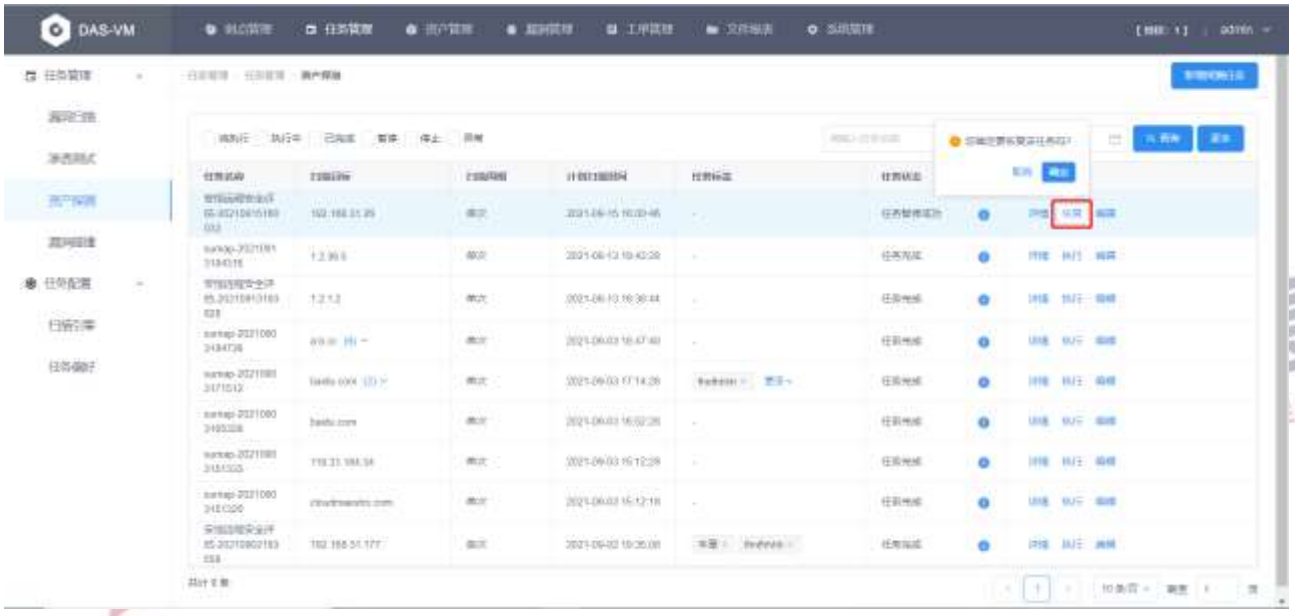


4.1.3.4. 探测任务暂停与恢复

（1） 点击任务列表操作列<暂停>按钮并确定，可暂停正在执行的探测任务。暂停任务成功后对应任务状态变更为任务暂停成功，右侧操作列栏按钮变为<详情>、<恢复>和<编辑>，<编辑>按钮置灰。

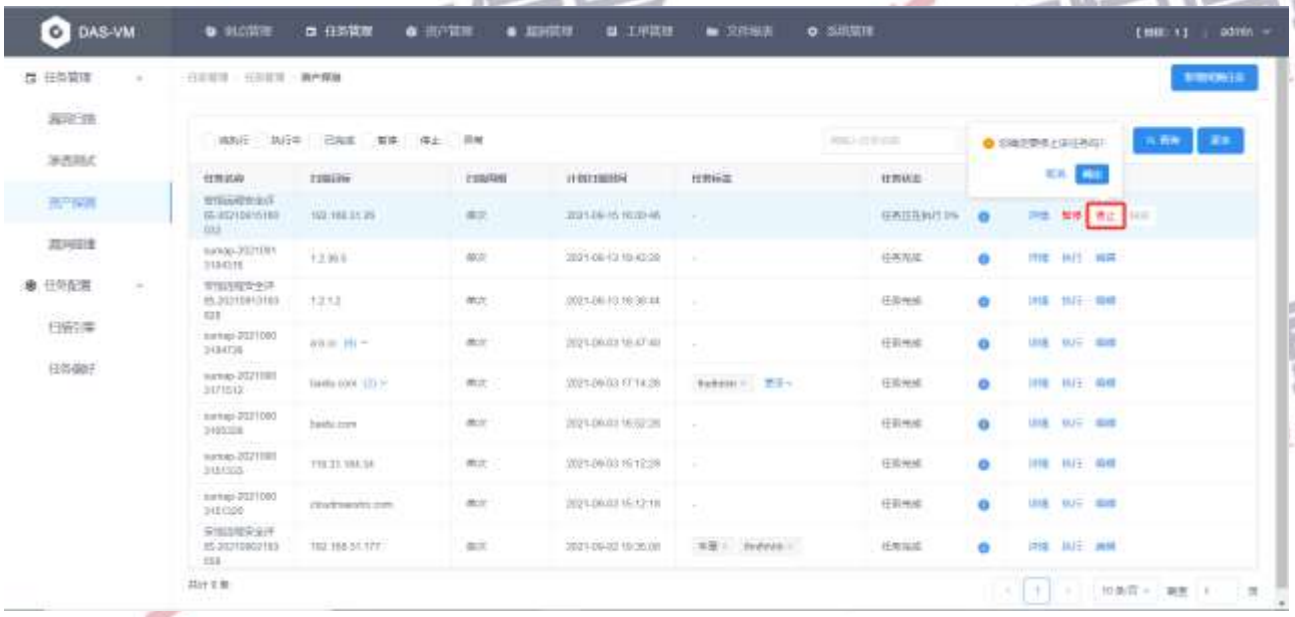


（2） 点击任务列表操作列<恢复>按钮并确定，可恢复暂停中的扫描任务，使其继续执行。



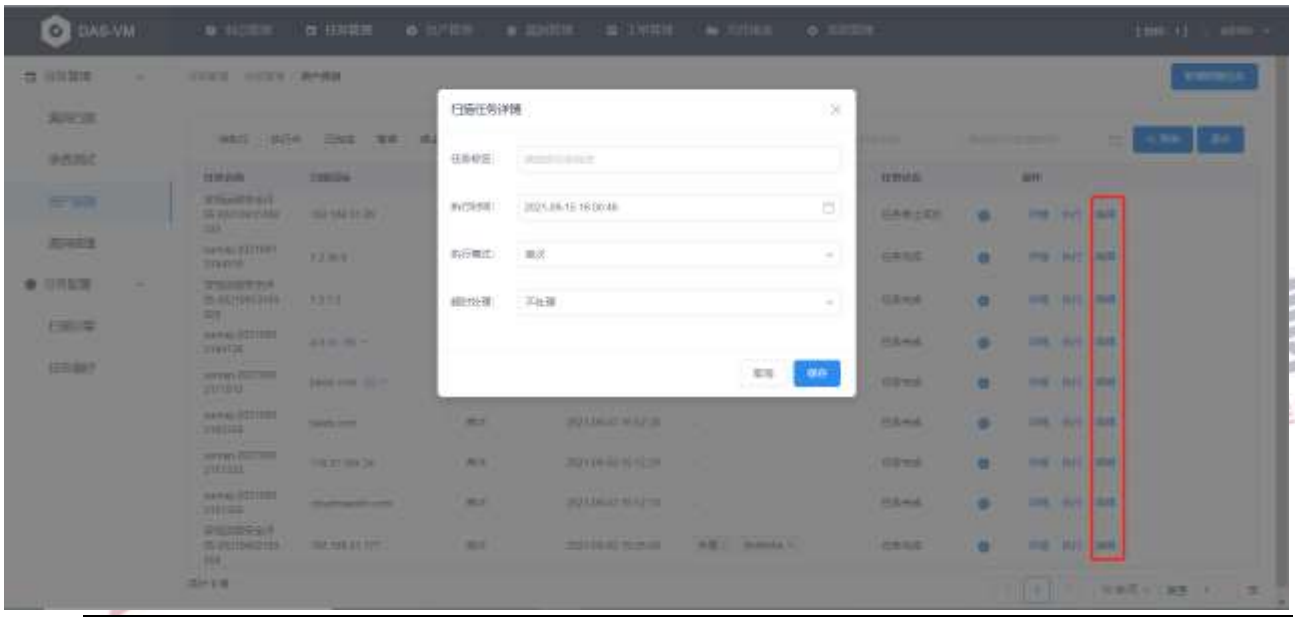
4.1.3.5. 探测任务停止

（1） 点击任务列表操作列<停止>按钮并确定，可停止正在执行的扫描任务。停止任务成功后对应任务状态变为任务停止成功，右侧操作栏按钮为<详情>、<执行>和<编辑>。



4.1.3.6. 探测任务编辑

（1） 点击<编辑>按钮，可以在探测任务详情编辑页面修改探测任务的任务标签、执行时间、执行方式、超时处理和超时时间。

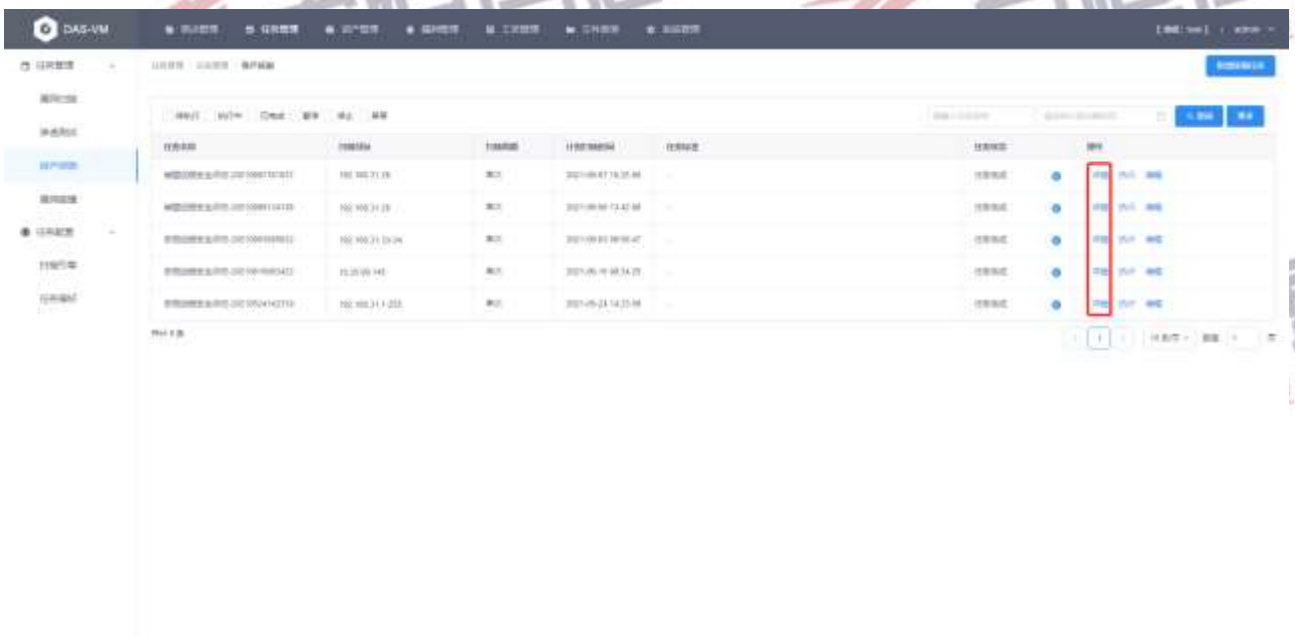


注意

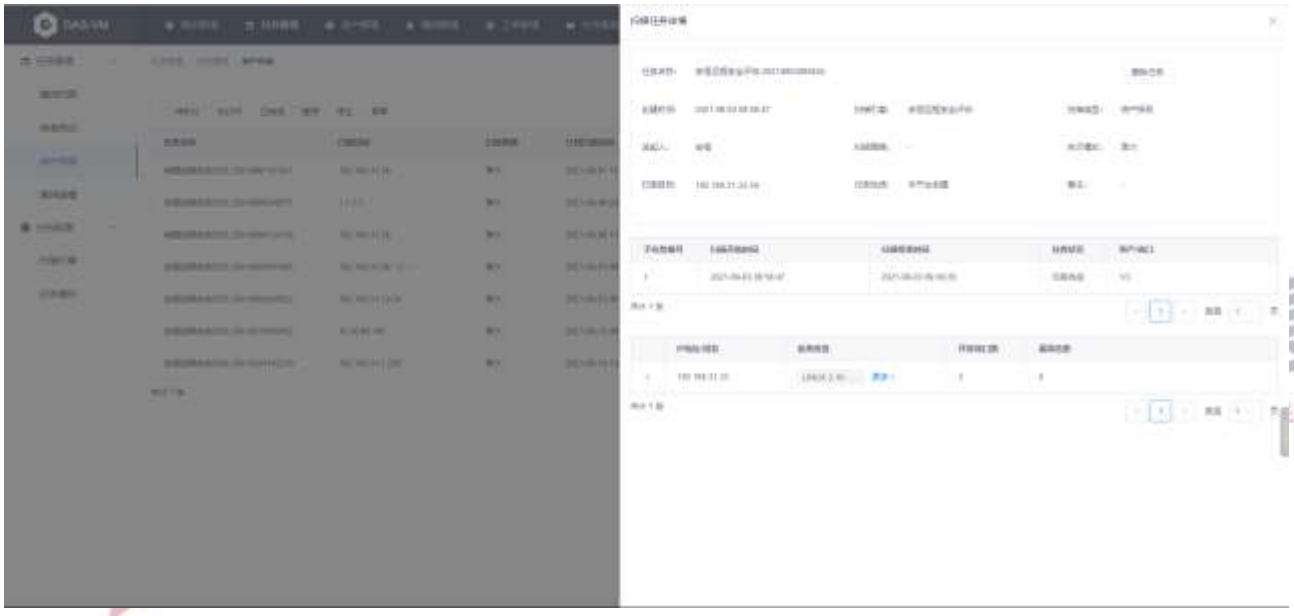
<编辑>按钮只能修改探测任务的任务标签、执行时间、执行方式、超时处理、超时时间。

4.1.3.7. 探测任务详情

（1） 点击探测任务列表中的<详情>按钮，可以查看该任务的任务详情。

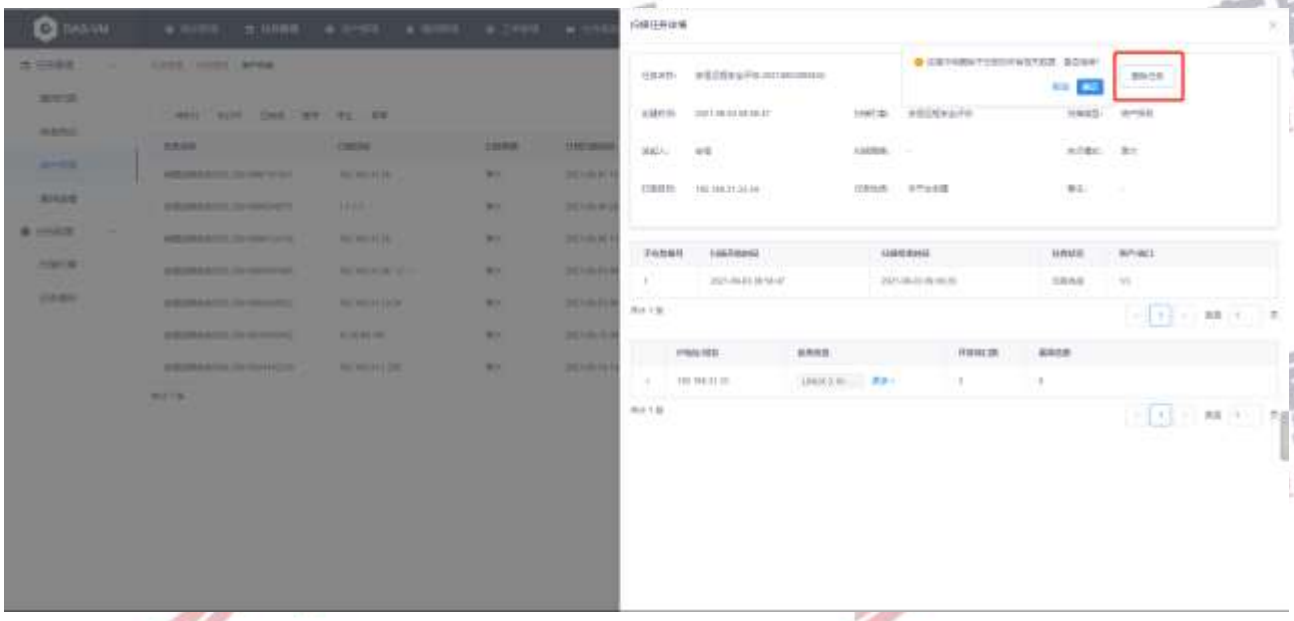


（2） 扫描任务详情可查看该任务的任务名称、扫描策略、扫描类型、扫描工具等任务信息以及各子任务扫描结果。



4.1.3.8. 探测任务删除

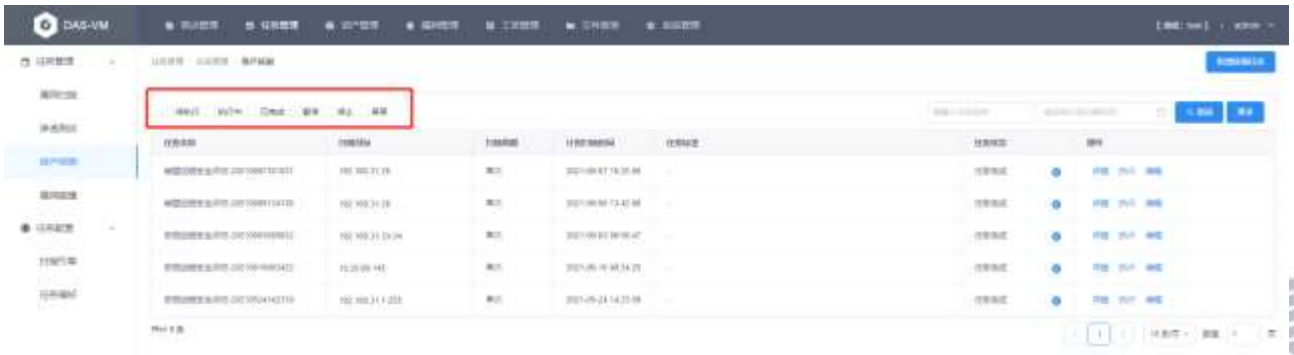
（1） 点击探测任务详情的右上角<删除任务>按钮并确认，可删除对应的探测任务。



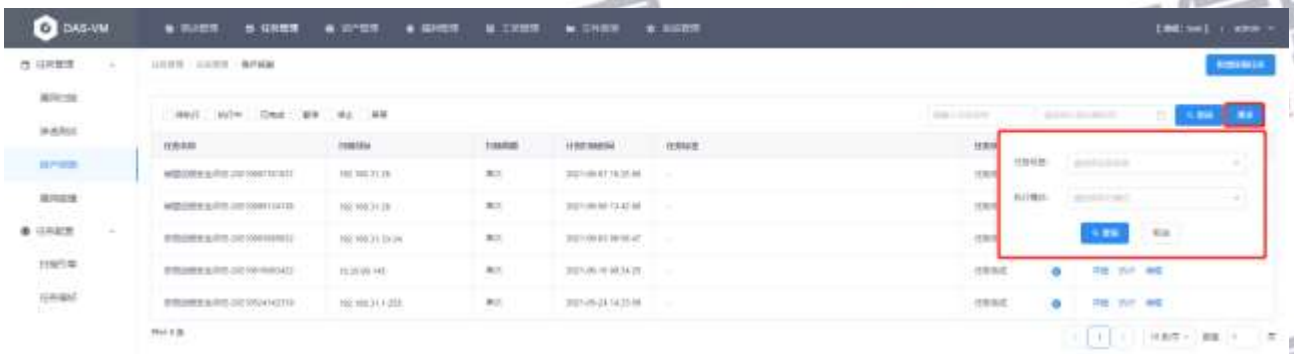
4.1.3.9. 探测任务查询

（1） 勾选页面中的任务完成情况：待执行、执行中、已完成、暂停、停止、异常，即可进行相应的扫描任务查询，具体完成情况细分如下：

- 待执行：当前尚未开始执行或正在等待调度的任务。
- 执行中：当前正在执行的扫描任务。
- 已完成：已经执行完成的扫描任务。
- 暂停：执行过程中被暂停的扫描任务。
- 停止：执行过程中被停止的扫描任务。
- 异常：执行过程中出现异常的扫描任务。



（2）选择查询时间、任务名称后，点击<查询>按钮进行任务查询，也可点击<更多>按钮，选择更多的查询条件，如：任务标签、扫描类型、执行方式。

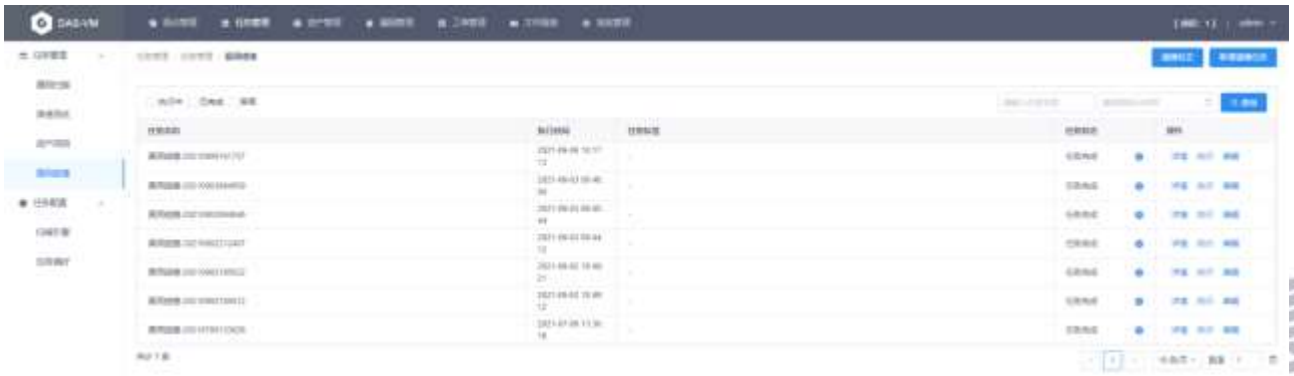


4.1.4. 漏洞碰撞

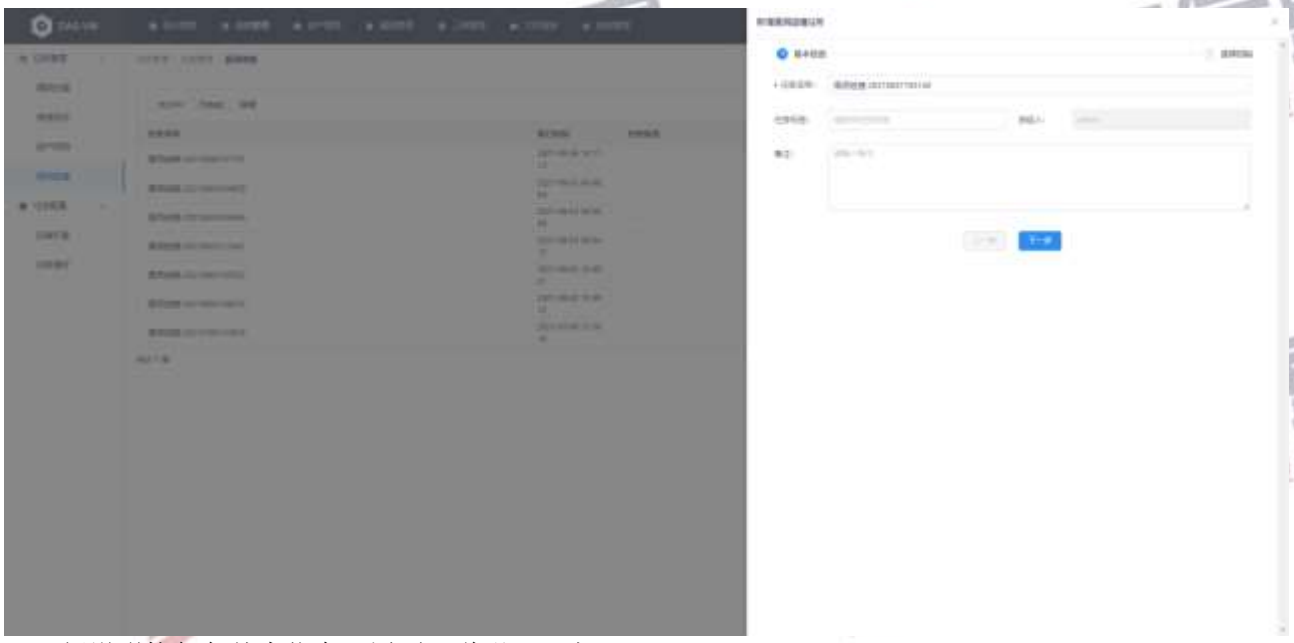
漏洞碰撞可以在平台漏洞库中查询影响实体生产厂商、型号、版本三个字段与碰撞目标匹配的漏洞，具体包括以下几个方面的内容：漏洞碰撞任务创建、执行和碰撞结果查看。

4.1.4.1. 碰撞任务新增

（1） 用户 WEB 登录后，进入[任务管理 /任务管理 /漏洞碰撞]页面。



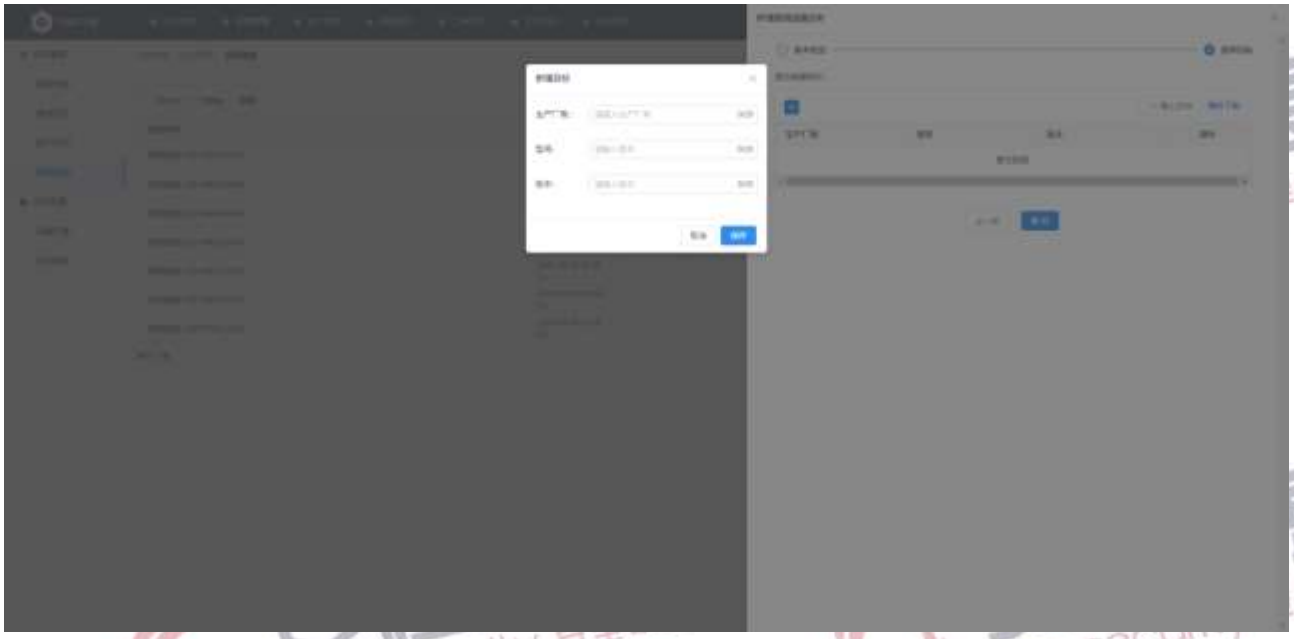
（2）点击右上角的<新增碰撞任务>按钮。弹出新增碰撞任务窗口，默认进入基本信息页面，选择任务标签，输入任务名称和备注。



新增碰撞任务基本信息配置项及说明见下表：

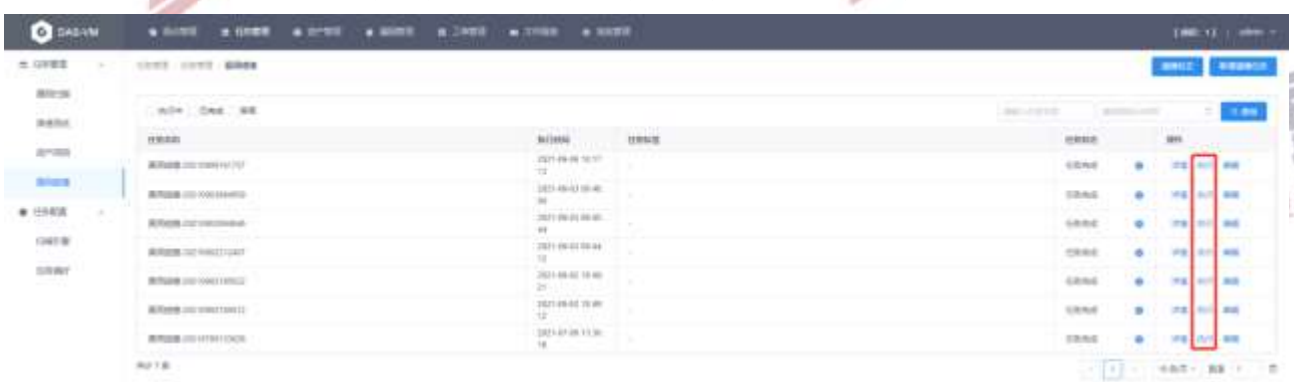
配置项	说明
任务名称	必填项。新增碰撞任务的任务名称。
任务标签	选填项。选择任务标签，将碰撞任务归类到对应个标签下。
发起人	必填项，置灰。默认创建碰撞任务的发起人，即当前登录用户。
备注	选填项。新增碰撞任务的注解说明。

（3） 点击<下一步>按钮进入选择目标页面，点击 增加碰撞目标，碰撞目标生产厂商、型号、版本三项至少选填一项，每项不超过 20 个字符，碰撞目标各字段输入时支持联想，联想范围取值于碰撞校正中对应字段的原始值。也可通过导入 excel 文件批量导入碰撞目标，点击<保存>按钮 ，碰撞任务创建完成。



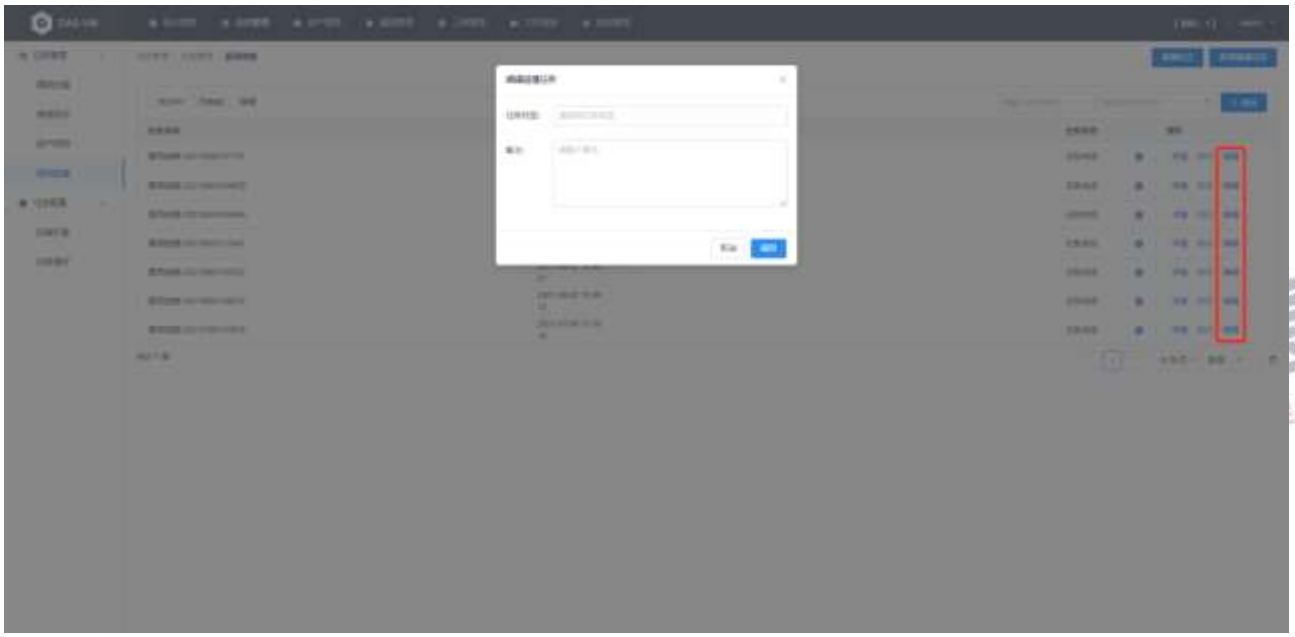
4.1.4.2. 碰撞任务执行

（1） 点击任务列表的<执行>按钮并确定，可立即执行一次对应的碰撞任务。



4.1.4.3. 碰撞任务编辑

（1） 点击<编辑>按钮，可以在碰撞任务详情编辑页面修改碰撞任务的任务标签和备注。

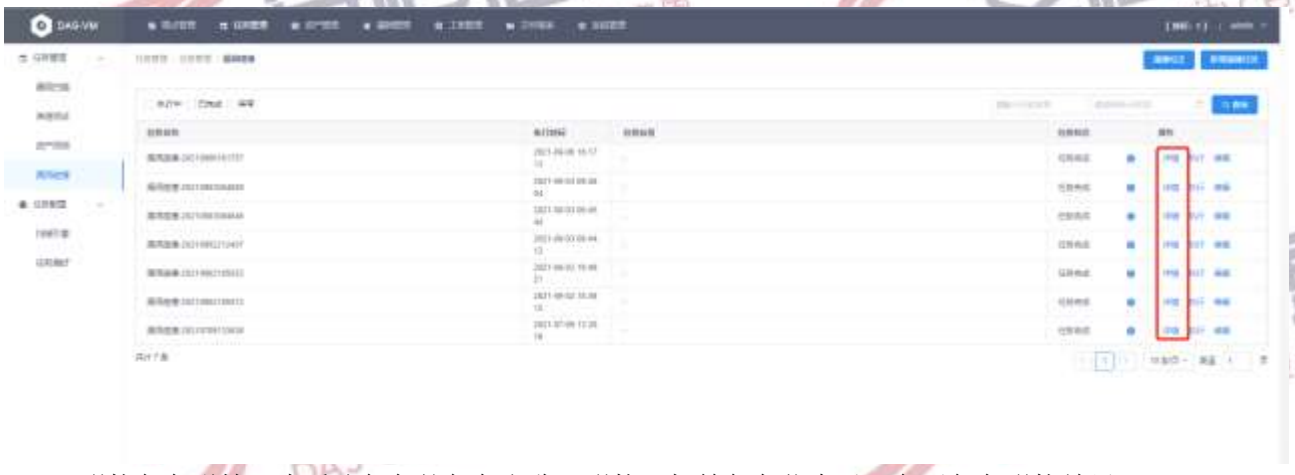


注意

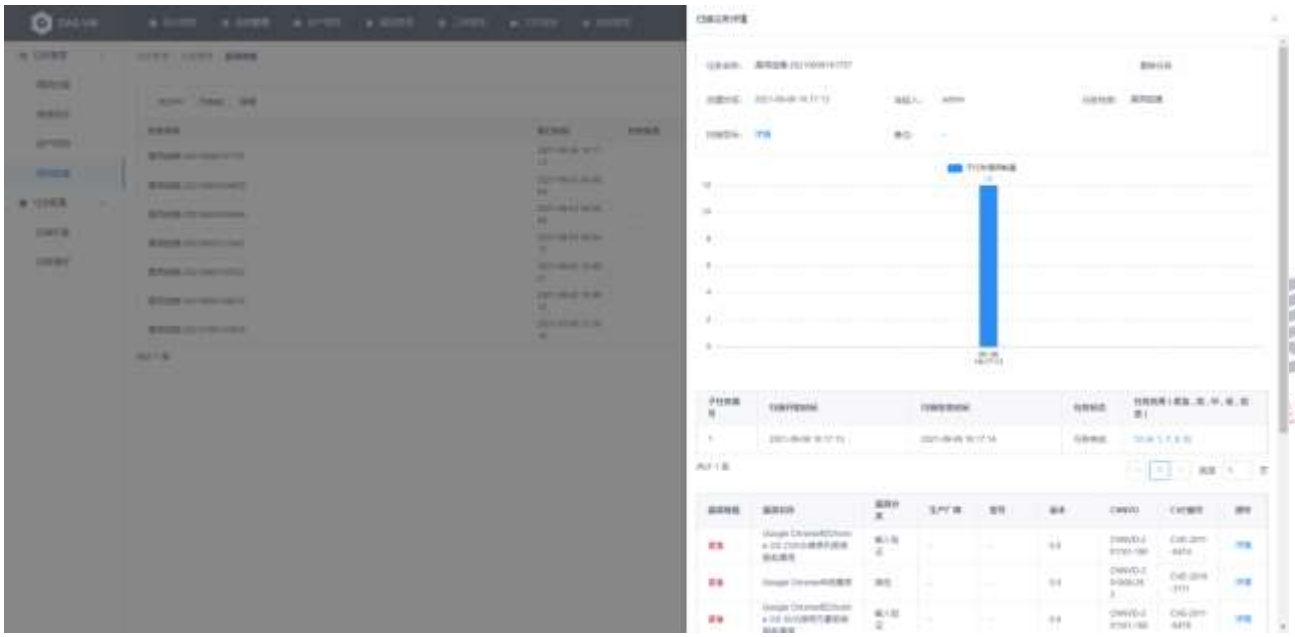
<编辑>按钮只能修改碰撞任务的任务标签和备注。

4.1.4.4. 碰撞任务详情

（1） 点击碰撞任务列表中的<详情>按钮，可以查看该任务的任务详情。

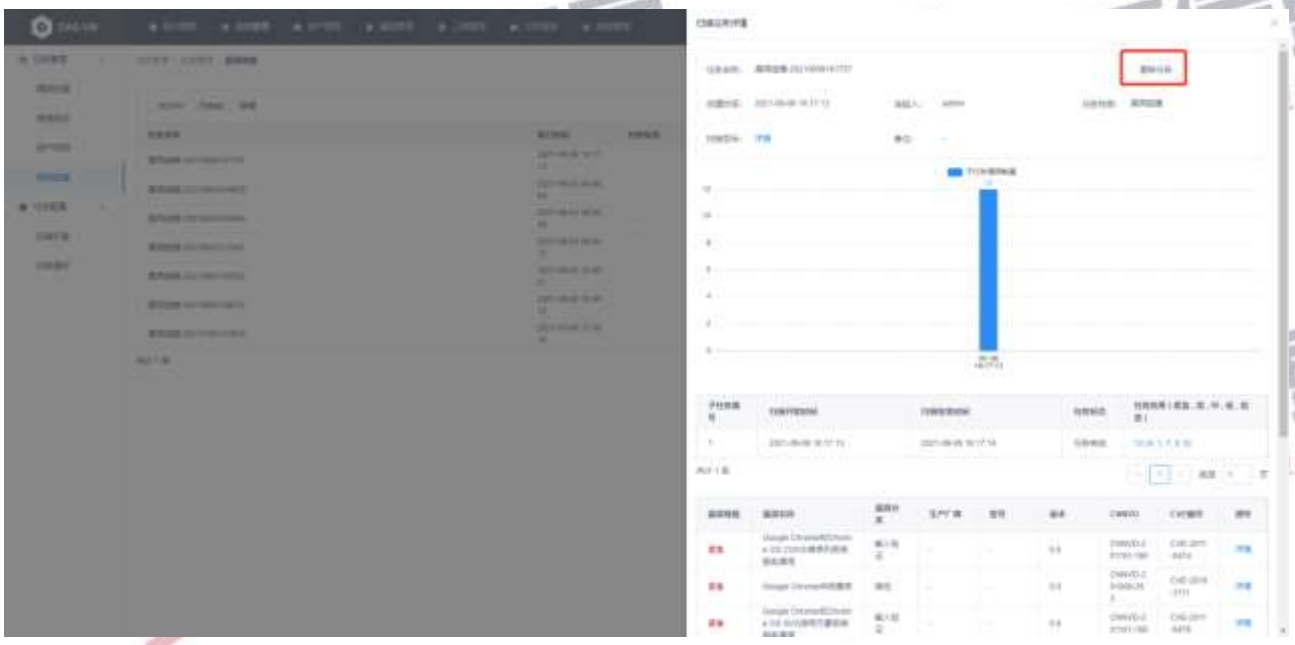


（2） 碰撞任务详情可查看该任务的任务名称、碰撞目标等任务信息以及各子任务碰撞结果。



4.1.4.5. 碰撞任务删除

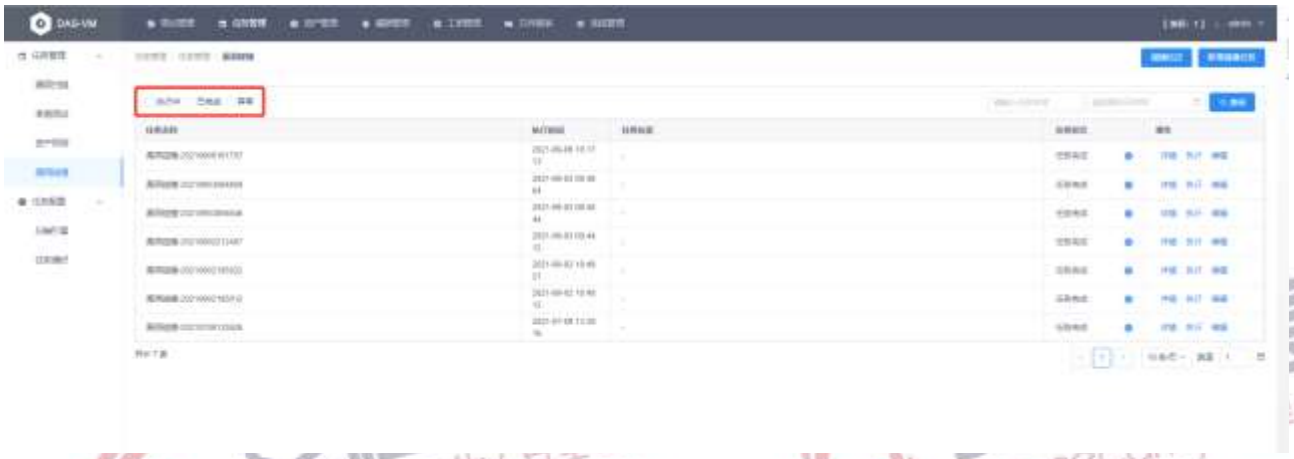
（1） 点击碰撞任务详情的右上角<删除任务>按钮并确认，可删除对应的碰撞任务。



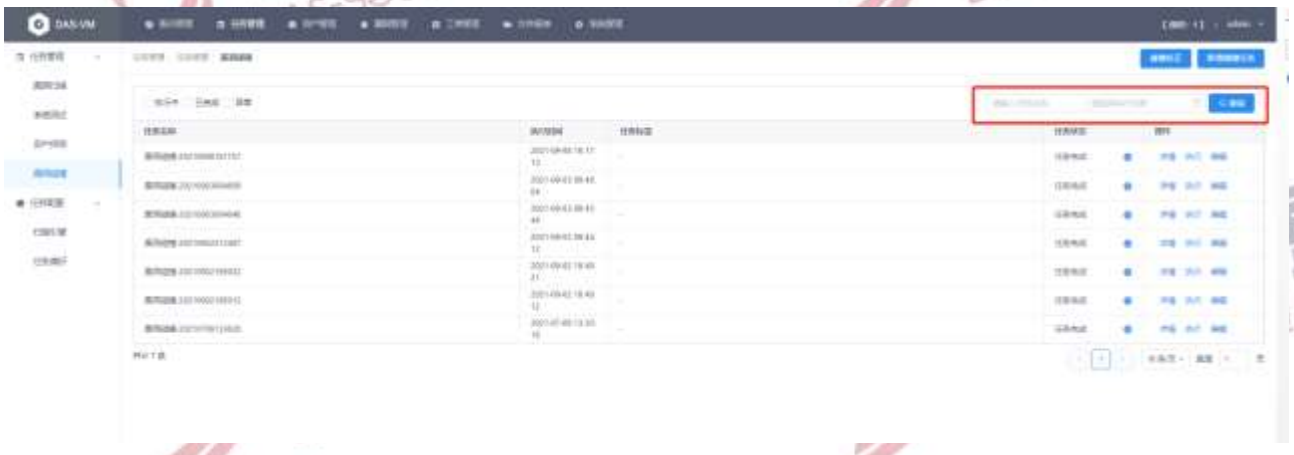
4.1.4.6. 碰撞任务查询

（1） 勾选页面中的任务完成情况：执行中、已完成、异常，即可进行相应任务状态的碰撞任务查询，具体完成情况细分如下：

- 执行中：当前正在执行的碰撞任务。
- 已完成：已经执行完成的碰撞任务。
- 异常：执行过程中出现异常的碰撞任务。



（2） 选择执行时间、任务名称后，点击<查询>按钮进行任务查询。

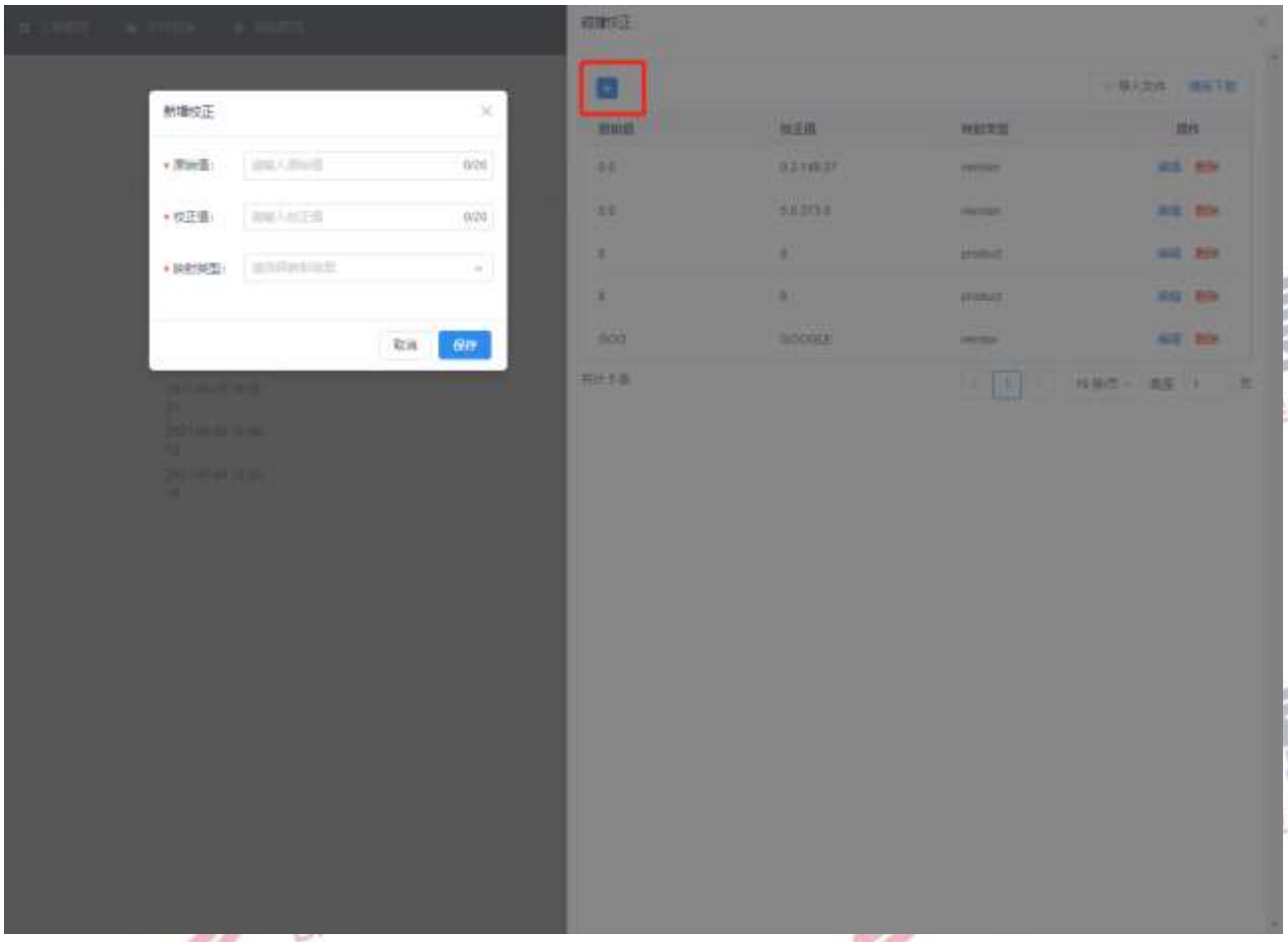


4.1.4.7. 碰撞校正

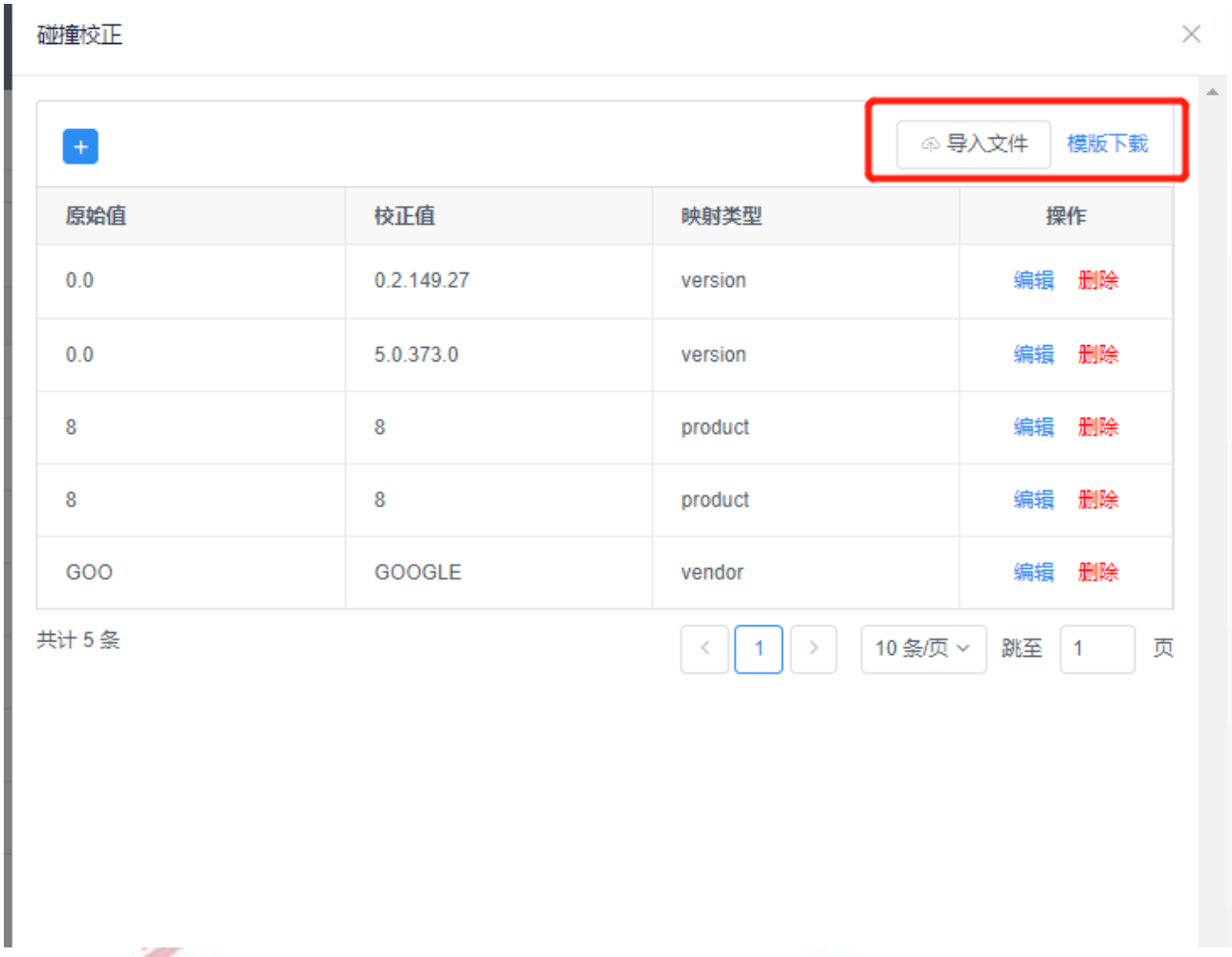
碰撞校正功能可把碰撞目标各字段的值按具体的映射类型转换为通用校正值后与漏洞库中影响实体的各字段值进行碰撞。

（1） 点击右上角的<碰撞校正>按钮，弹出碰撞校正窗口。

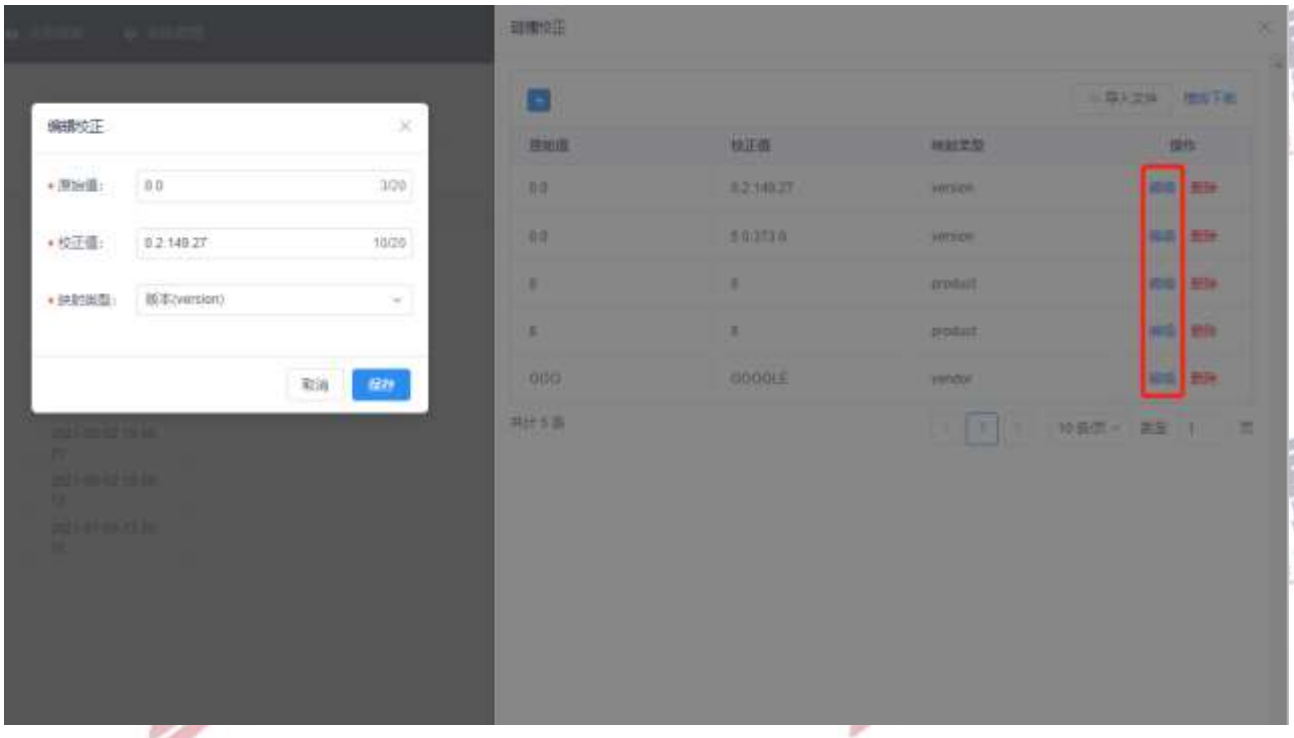
（2） 点击  弹出新增校正窗口，输入原始值、校正值、映射类型，原始值和校正值每项不超过 20 个字符点击<保存>按钮 ，碰撞任务创建完成。



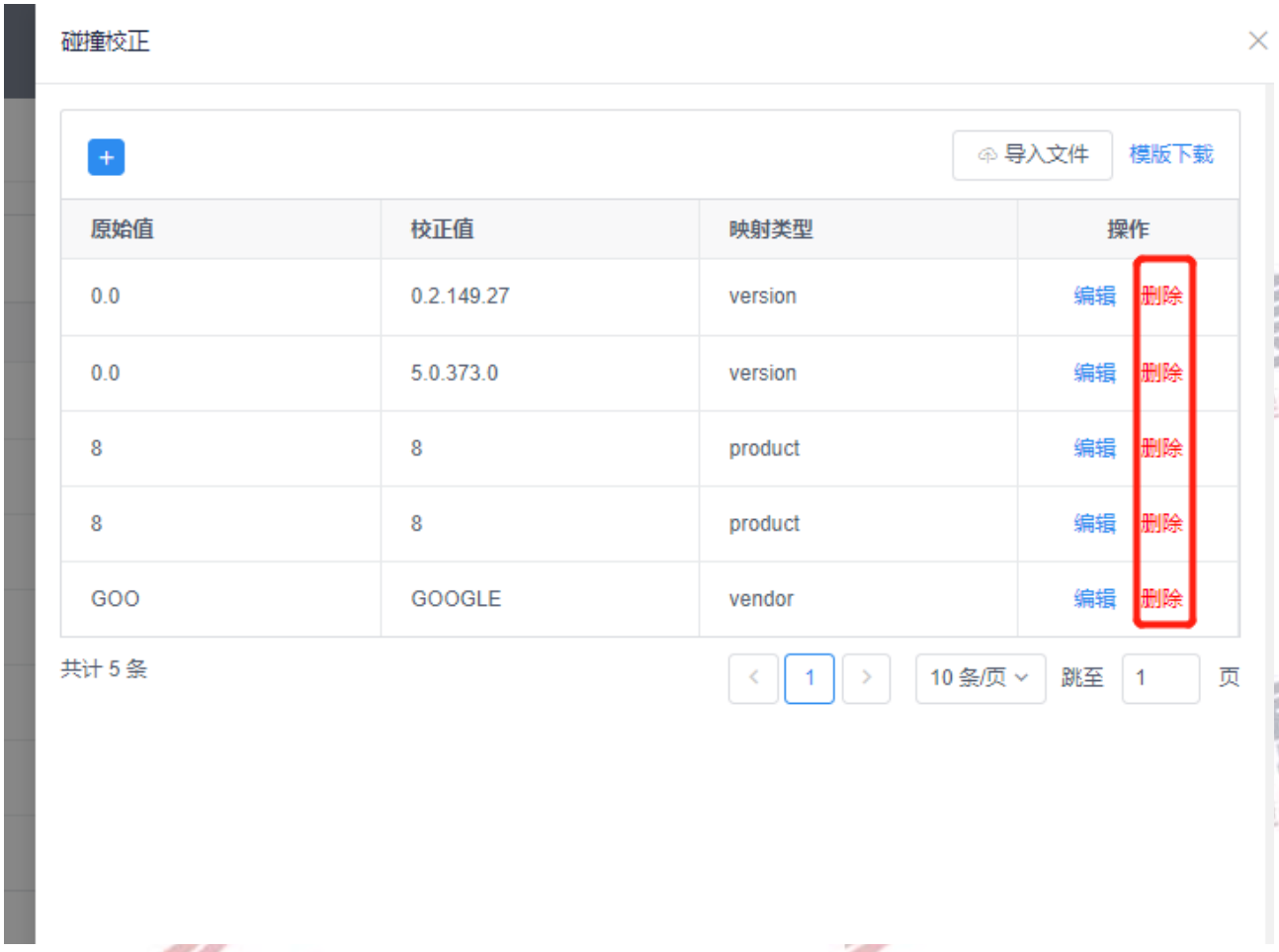
（3） 也可通过点击<模板下载>按钮下载模板，编辑后点击<导入文件>按钮批量导入校正规则。



（4）点击<编辑>按钮，可以修改对应的校正规则。



（5）点击<删除>按钮并确定，可以删除对应的校正规则。



4.2. 任务配置

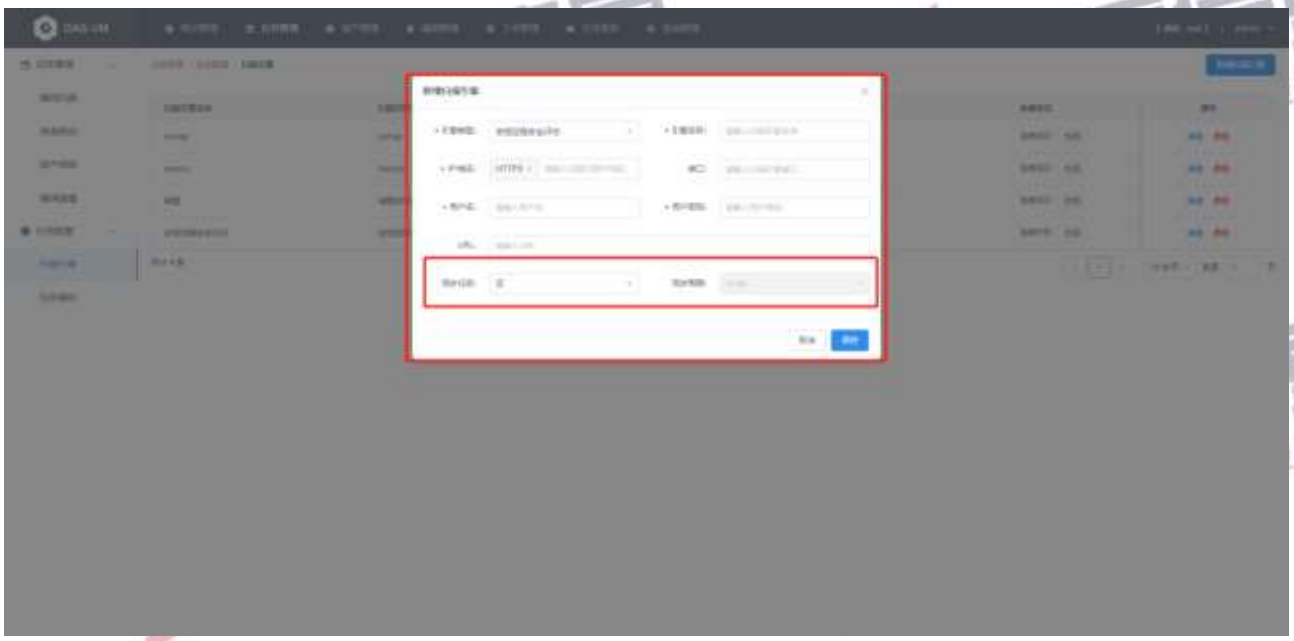
4. 2. 1. 扫描引擎

扫描引擎页面主要用于自动化漏洞扫描平台的扫描引擎对接配置，安恒远程安全评估、绿盟远程安全评估、Nessus 扫描引擎的名称、IP 和端口具有唯一性，sumap 扫描引擎的名称具有唯一性。

4.2.1.1. 新增扫描引擎

（1） 用户 WEB 登录后，进入[任务管理/任务配置/扫描引擎]页面。

（2）点击<新增扫描引擎>按钮 ，弹出新增扫描引擎窗口，填写相应的信息，点击<保存>按钮，即可完成扫描引擎添加。



扫描引擎配置项及说明见下表：

配置项	说明
扫描引擎名称	必填项。新增扫描引擎的名称。
扫描引擎类型	必填项。新增扫描引擎的类型，有安恒远程安全评估和绿盟远程安全评估。
IP/域名	必填项。新增扫描引擎的 ip/域名地址。
端口	选填项。新增扫描引擎的扫描端口。

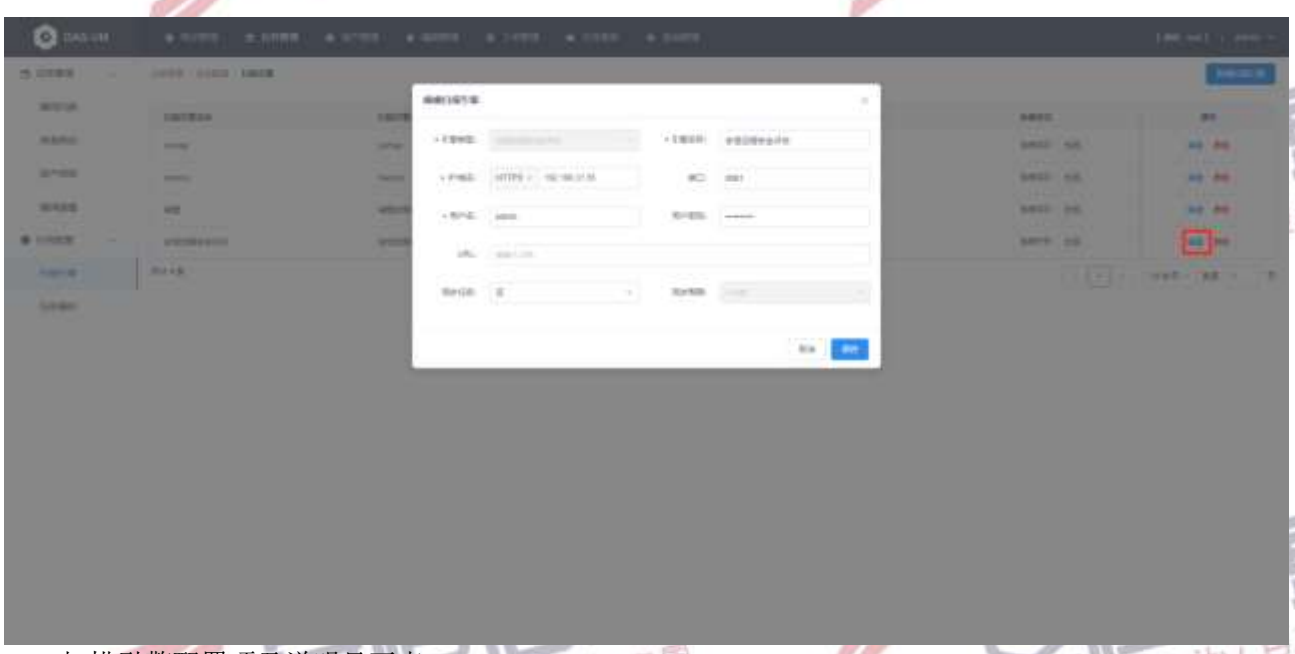
用户名	必填项。新增扫描引擎所属的用户。
用户密码	必填项。新增扫描引擎所属用户的密码。
URL	选填项。新增扫描引擎的 URL 链接，可用于页面快速跳转
同步任务	选填项。新增安恒远程安全评估引擎的是否同步任务选项。
同步周期	选填项。新增安恒远程安全评估引擎的同步周期。

Sumap 扫描引擎仅支持资产探测，相关配置项及说明见下表

配置项	说明
引擎类型	必填项。新增扫描引擎的类型。
引擎名称	必填项。新增引擎名称。
Token	必填项。新增 sumap 扫描引擎的 Token。

4.2.1.2. 编辑扫描引擎

（1） 点击扫描引擎列表中的<编辑>按钮，弹出编辑扫描引擎窗口，修改相应的配置项信息，点击<保存>按钮，即可完成扫描引擎编辑。



扫描引擎配置项及说明见下表：

配置项	说明
扫描引擎名称	必填项。扫描引擎的名称。

扫描引擎类型	必填项。扫描引擎的类型，有安恒远程安全评估和绿盟远程安全评估。
IP/域名	必填项。扫描引擎的 ip 地址，增加 HTTP 和 HTTPS 选择。
端口	选填项。扫描引擎的扫描端口。
用户名	必填项。扫描引擎所属的用户。
用户密码	必填项。扫描引擎所属用户的密码。
URL	选填项。扫描引擎的 URL 链接，可用于页面快速跳转
同步任务	选填项。安恒远程安全评估扫描引擎是否同步任务。
同步周期	选填项。安恒远程安全评估扫描引擎的同步周期。
Token	必填项。sumap 扫描引擎的 Token。

4.2.1.3. 删除扫描引擎

（1） 点击扫描引擎列表中的<删除>按钮并确定，即可删除列表中的相应扫描引擎。

4.2.1.4. 检测扫描引擎

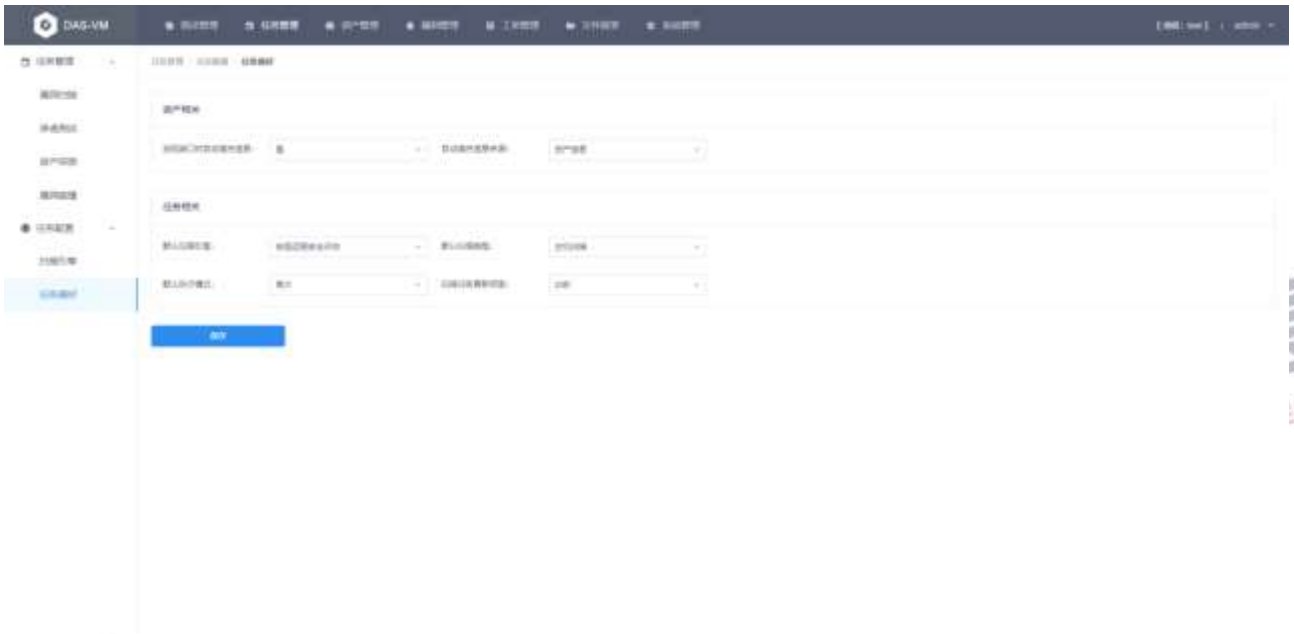
（1） 点击扫描引擎列表中连接状态旁的<检测>按钮，检测扫描引擎连接状况。

4. 2. 2. 任务偏好

主要用于设置系统扫描任务相关的一些默认配置，包括：资产相关、任务相关。

4.2.2.1. 资产相关

（1） 用户 WEB 登录后，进入[任务管理/任务配置/任务偏好]页面，显示默认的偏好设置信息



（2）设置与资产相关的默认配置，包括发现资产时是否自动填充信息、自动填充信息来源等，点击<保存>按钮，保存相关配置信息。

资产相关偏好设置配置项及说明见下表：

配置项	说明
发现资产时是否自动填充信息	设置是否自动填充信息
自动填充信息来源	设置信息来源包括：资产信息、端口信息

4.2.2.2. 任务相关

（1）设置与扫描任务相关的默认配置，包括默认扫描引擎、默认扫描类型、默认执行方式、扫描任务更新频率等，点击<保存>按钮，保存相关配置信息。

任务相关偏好设置配置项及说明见下表：

配置项	说明
默认扫描引擎	设置新增扫描任务时默认使用的扫描引擎。
默认扫描方式	设置新增扫描任务时默认的扫描类型，包括：主机扫描、web 扫描、基线扫描、弱口令扫描、数据库扫描。
默认扫描执行模式	设置新增扫描任务时默认的扫描任务执行模式，包括：单次执行、每天执行、每周执行、每月执行、每年执行。
扫描任务更新频率	设置扫描任务状态默认更新频率，包括：20 秒、30 秒、1 分钟。

5. 资产管理

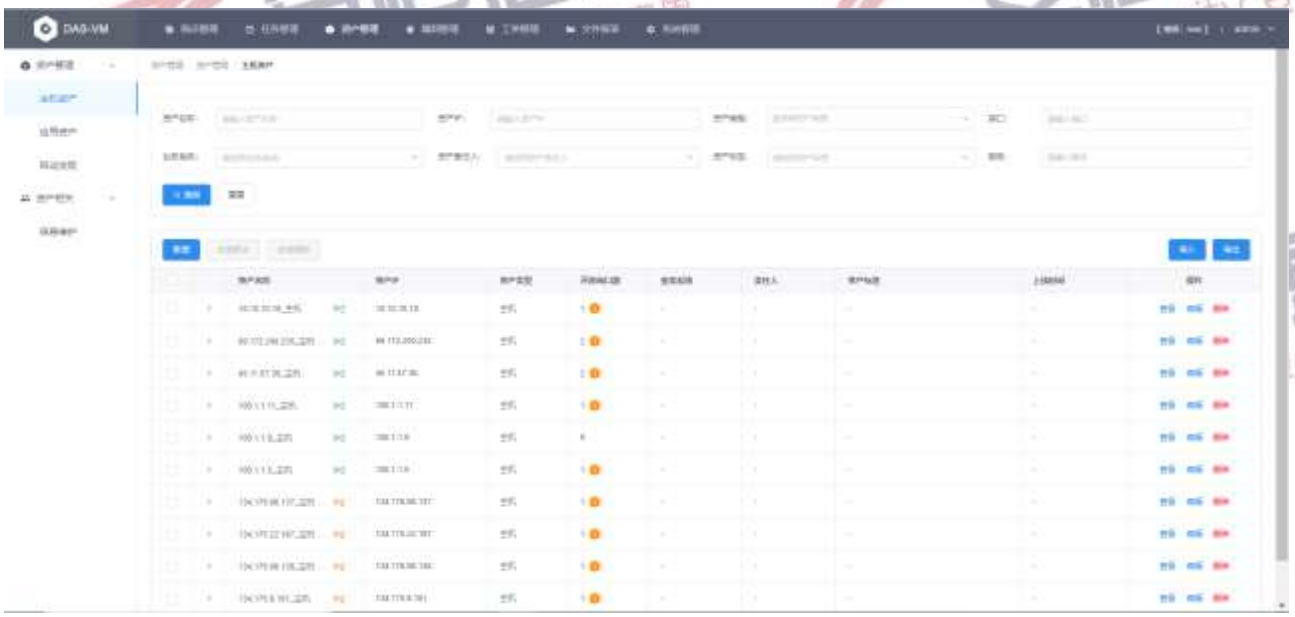
5.1. 资产管理

5. 1. 1. 主机资产

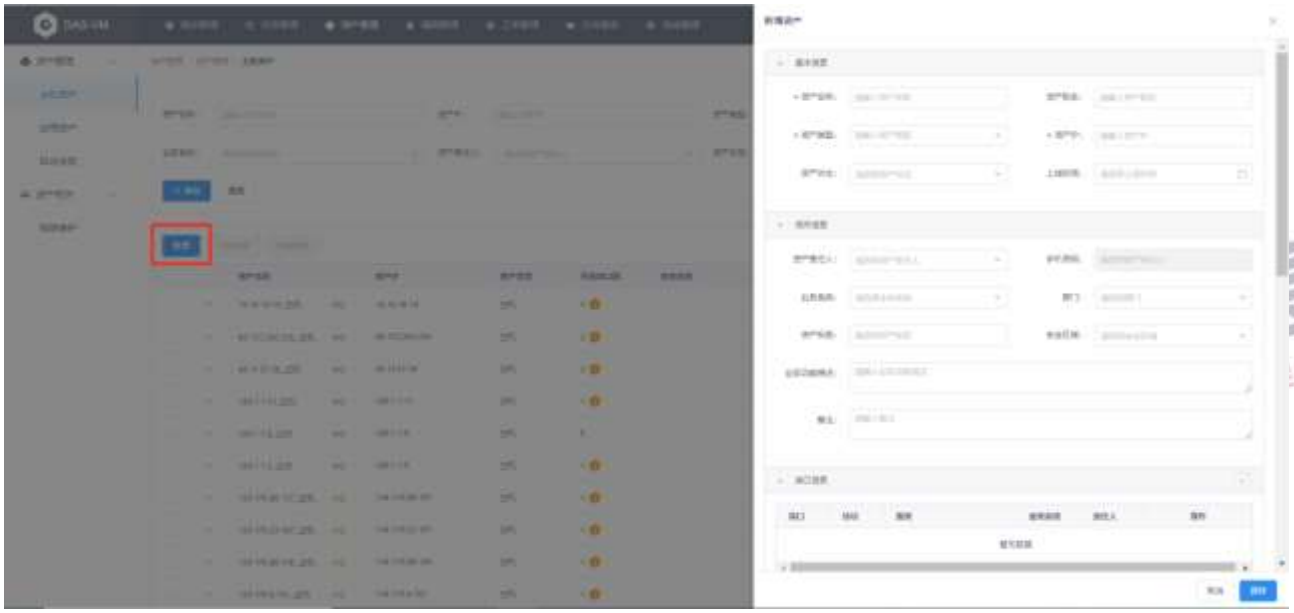
管理所有主机类型资产。

5.1.1.1. 新增资产

（1） 用户 WEB 登录后，进入[资产管理/资产管理/主机资产]页面。



（2） 点击<新增>按钮，进入新增主机资产页面，填写对应的资产信息，点击<保存>按钮，即可完成资产新增。



主机资产配置项及说明见下表：

配置项	说明
资产名称	必填项。新增资产的名称。
资产别名	选填项。新增资产的别名。
资产类型	必填项。主要有以下分类：主机、windows、Nix、应用类、安全类、网络类、审计组件和其他设备
资产 IP	必填项。新增资产的 IP 地址。
资产状态	选填项。选择新增资产状态。
上线时间	选填项。新增资产的上线时间。
业务系统	选填项。新增资产所属的业务系统。
资产责任人	选填项。新增资产的负责人。
手机号码	选填项，置灰。所选择的资产责任人的手机号码。
资产标签	选填项。新增资产的标签，资产标签选择框内点击添加标签，选择资产标签分类，输入标签名称快速完成资产标签添加，所添加的资产标签重要性为 1。当无资产标签分类时，快速添加资产标签时默认增加名称为“资产”、重要性为 1 的资产标签分类。
部门	选填项。新增资产的部门。
安全区域	选填项。新增资产的安全区域。

业务功能描述	选填项。新增资产的业务功能描述。
备注	选填项。新增资产的备注。
资产价值	新增资产的资产价值，资产价值由保密性、完整性、可用性、业务相关性四个属性决定。
保密性	选填项。新增资产的保密性，取值范围为 0~10，0 的重要性最低，10 的重要性最高，保留一位小数。
完整性	选填项。新增资产的完整性，取值范围为 0~10，0 的重要性最低，10 的重要性最高，保留一位小数。
可用性	选填项。新增资产的可用性，取值范围为 0~10，0 的重要性最低，10 的重要性最高，保留一位小数。
业务相关性	选填项。新增资产的业务相关性，取值范围为 0~10，0 的重要性最低，10 的重要性最高，保留一位小数。
资产重要性	必填项。新增资产的重要性，从 1 到 10 划分，1 的重要性最低，10 的重要性最高。
系统信息	选填项。新增资产的系统信息，可以填写操作系统、系统版本和软件版本等相关信息。通过输入标签名称快速完成系统信息标签添加，添加的系统信息标签可以快速进行修改和删减。
主机名	选填项。新增资产的主机名。
MAC 地址	选填项。新增资产的物理地址。
物理位置	选填项。新增资产的物理位置。
逻辑位置	选填项。新增资产的逻辑位置。
远程管理方式	选填项。新增资产的远程管理方式。
设备厂商	选填项。新增资产的设备厂商。
设备型号	选填项。新增资产的设备型号。
设备版本	选填项。新增资产的设备版本。
机房 IDC	选填项。新增资产的机房 IDC。
服务供应商 ISP	选填项。新增资产的服务供应商 ISP。
自治系统号 ASN	选填项。新增资产的自治系统 ASN。
国家	选填项。新增资产的国家。

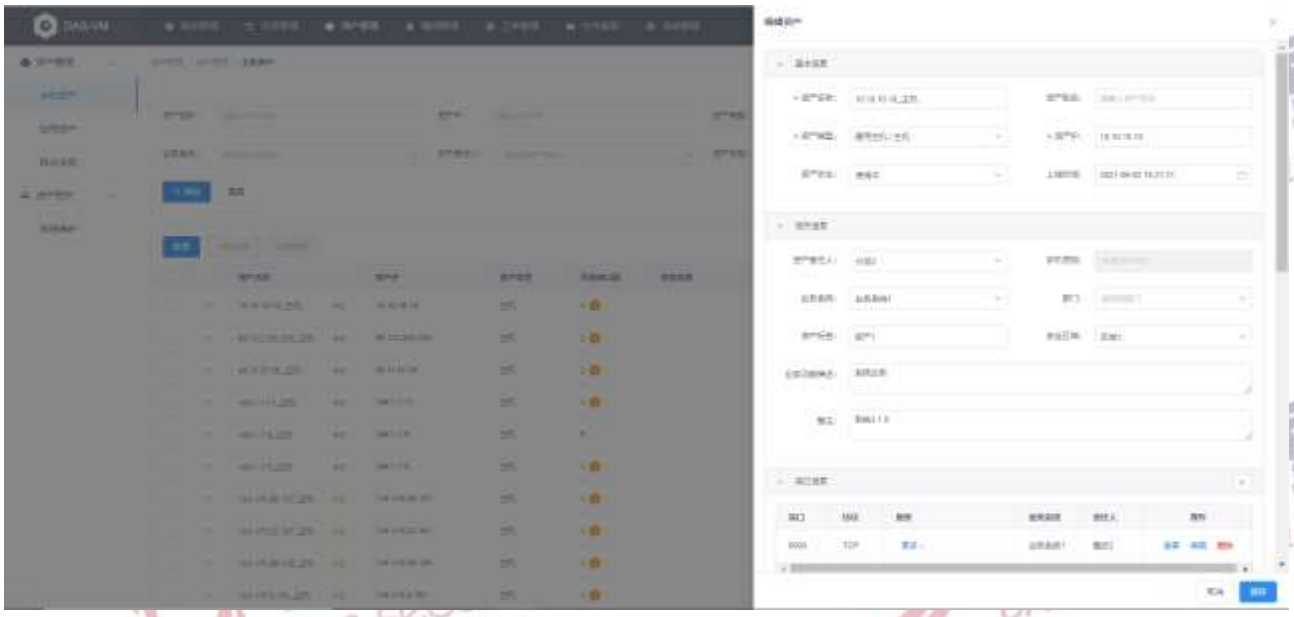
省份	选填项。新增资产的省份。
城市	选填项。新增资产的城市。
所有者	选填项。新增资产的所有者。
经度	选填项。新增资产的经度。
纬度	选填项。新增资产的纬度。

注意

带有“*”号的必须填写，才能成功添加资产

5.1.1.2. 查看资产

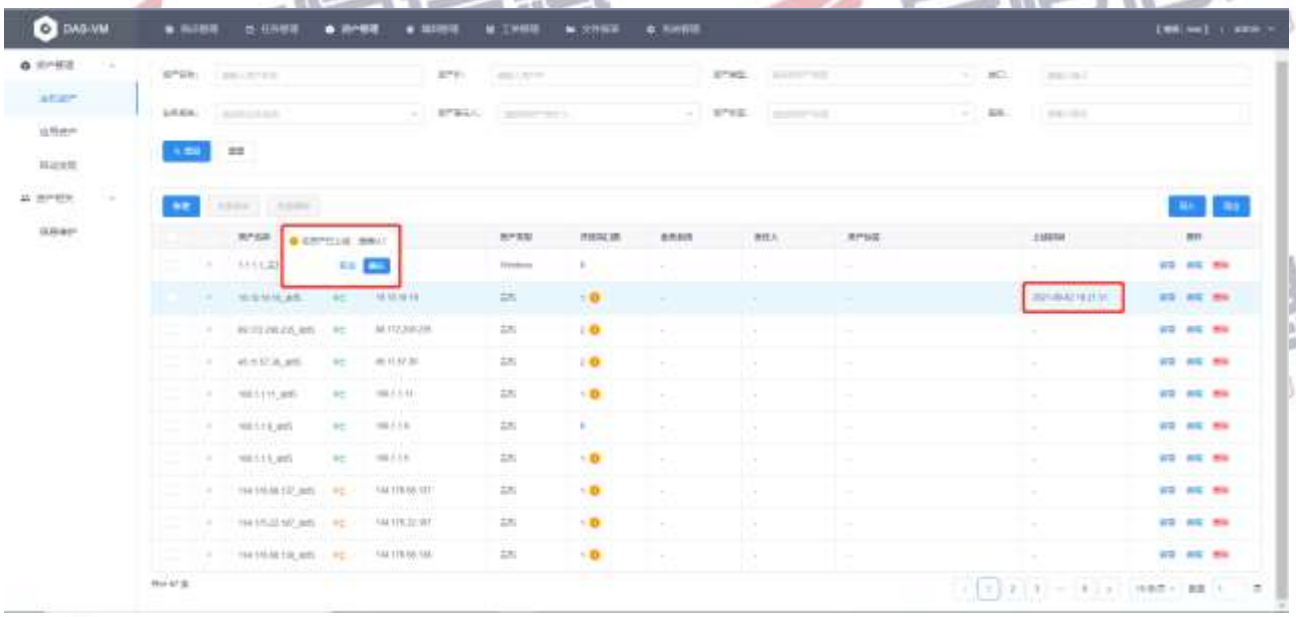
（1） 点击主机资产列表的<查看>按钮，进入资产详情页面，查看资产信息和相关配置信息。



5.1.1.3. 资产上下线告警

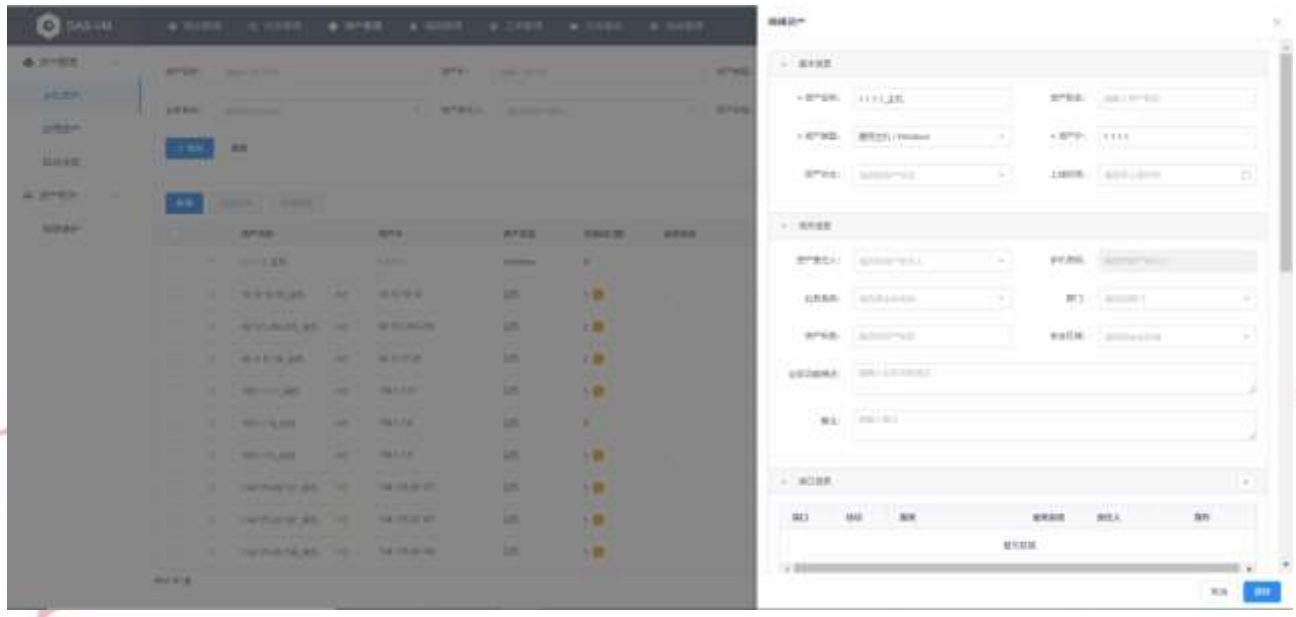
（1）资产扫描后，当主机资产存在开放端口时显示上线图标，当主机资产不存在开放端口时显示下线图标。

（2）点击上线图标可进行上线确认，确认后对应资产上线时间变更为确认时间。

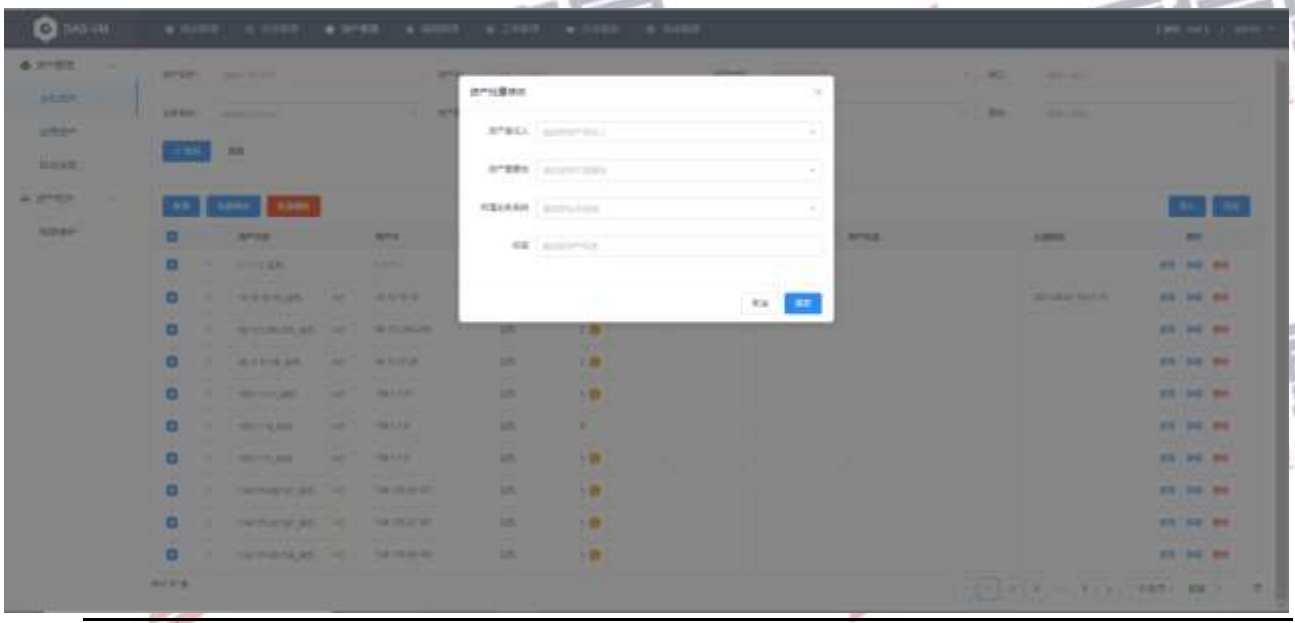


5.1.1.4. 编辑资产

（1） 点击主机资产列表的<编辑>按钮，进入资产编辑页面，修改资产信息后，单击<保存>按钮，即可完成资产编辑。



（2）勾选多个资产后，点击<批量修改>按钮，进入资产批量修改页面，修改资产信息后，单击<保存>按钮，即可完成资产的批量编辑。

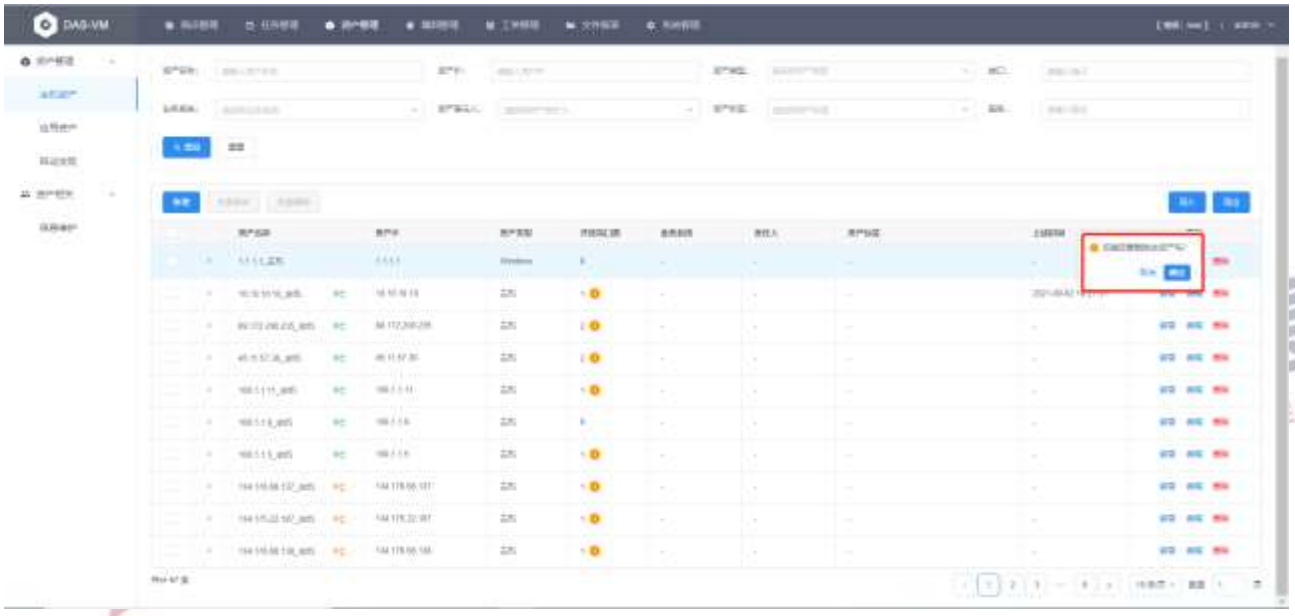


注意

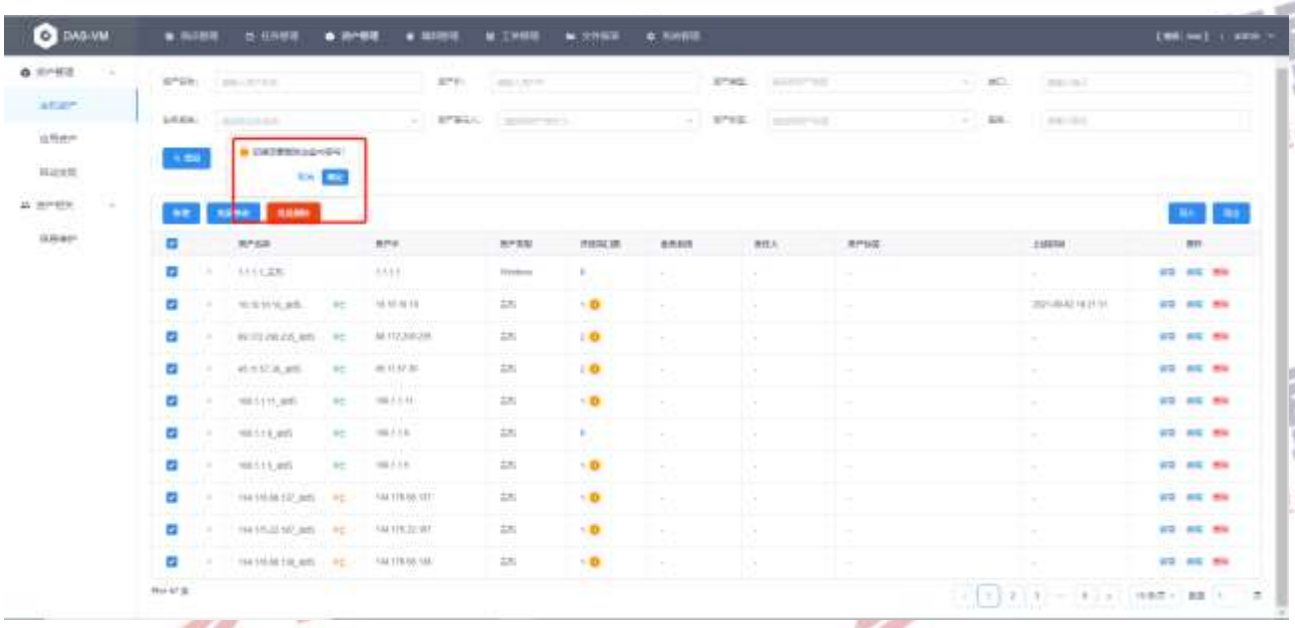
批量修改只能修改资产的资产负责人、资产重要性、所属业务系统和资产标签这四项。

5.1.1.5. 删除资产

（1） 点击主机资产列表的<删除>按钮并确定，可删除对应资产的资产信息和相关配置信息。

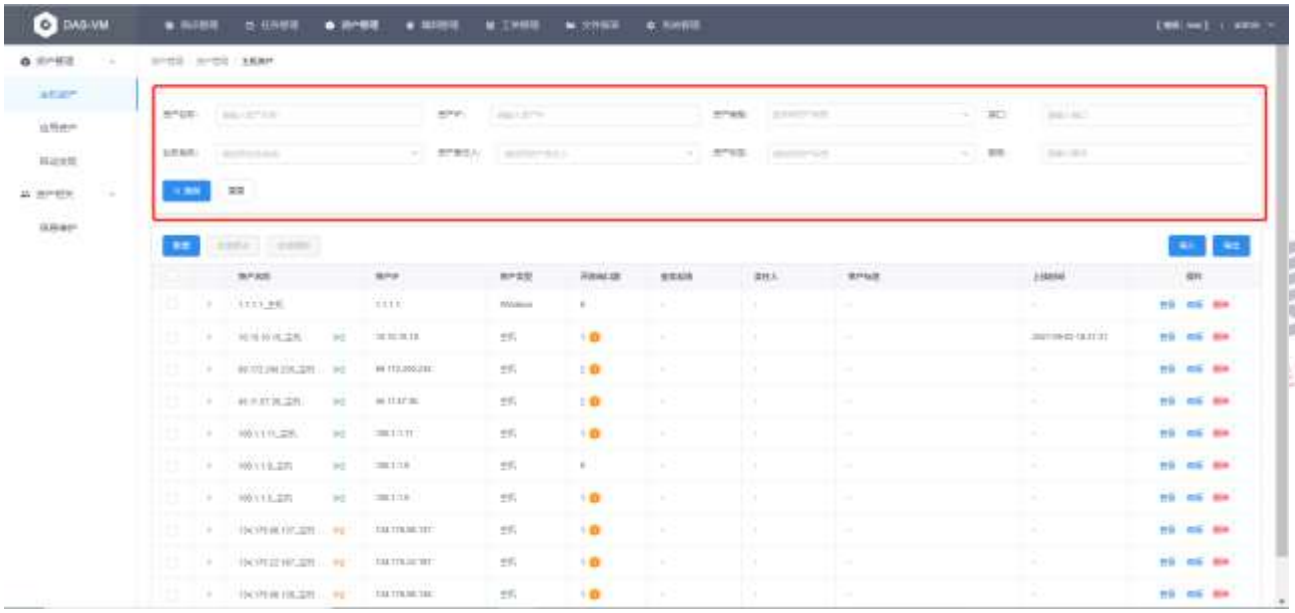


（2）勾选多个资产后，点击<批量删除>按钮并确认，即可删除勾选的多个资产。



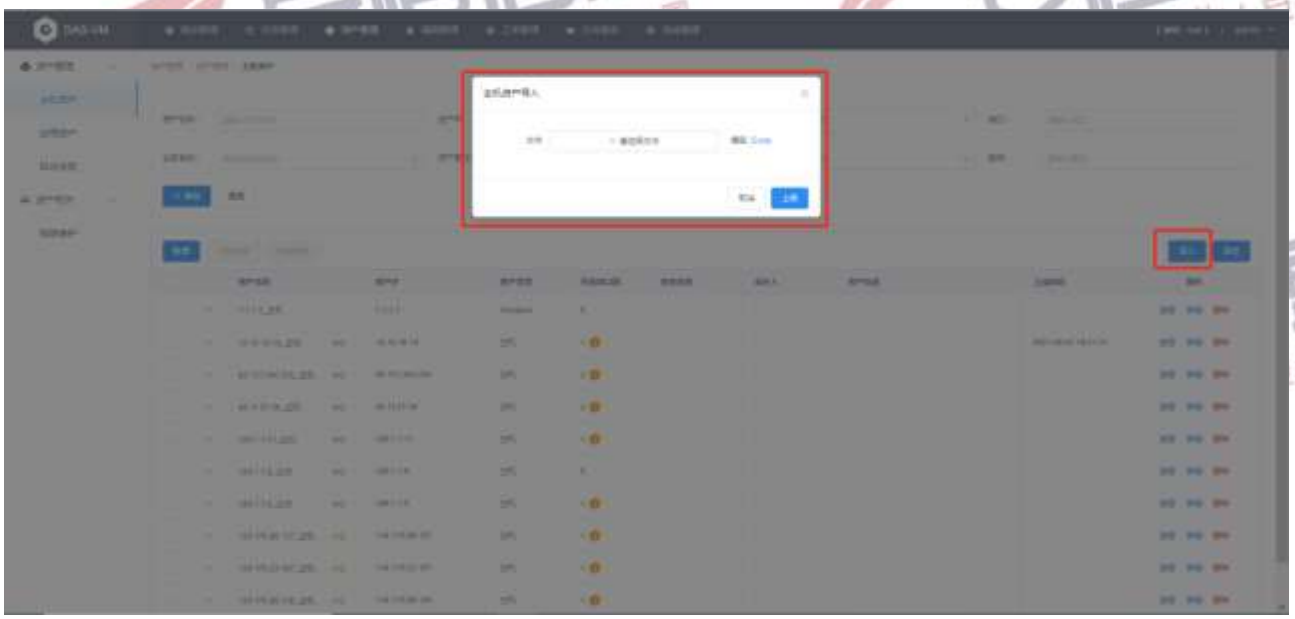
5.1.1.6. 查询资产

（1） 设置查询条件，可在主机资产列表中进行指定资产查询，条件设置后，点击<查询>按钮，进行查询。点击<重置>按钮，可清空查询条件。

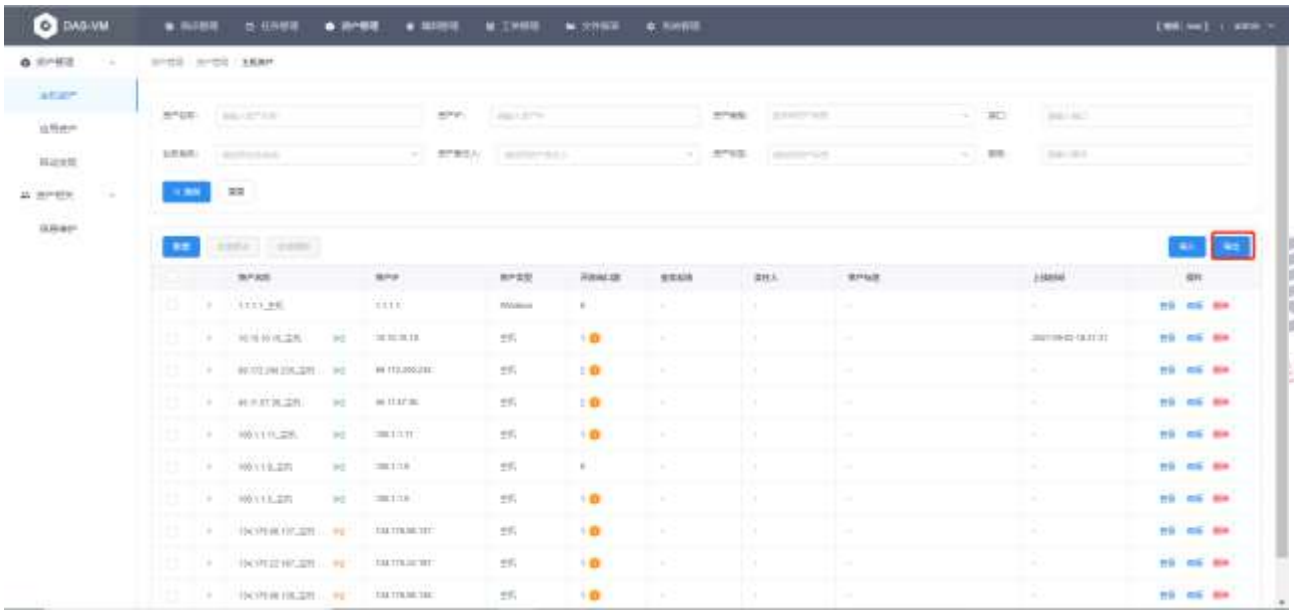


5.1.1.7. 导入导出

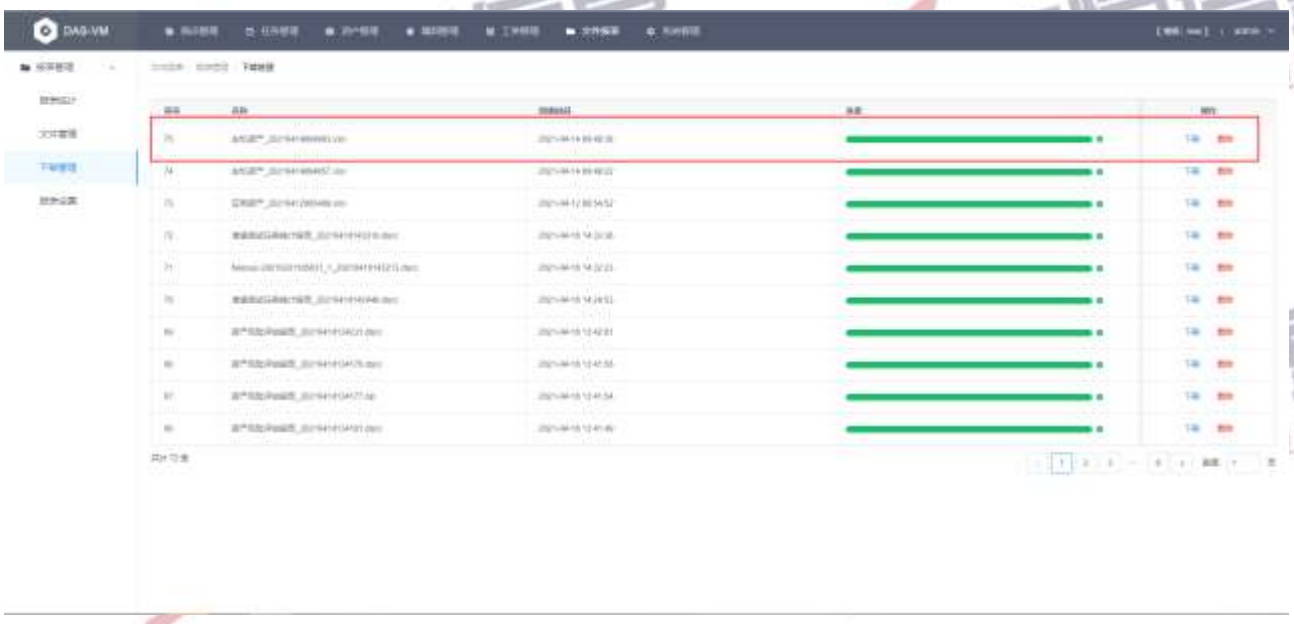
（1） 点击<导入>按钮，选择 excel 文件后，点击<上传>按钮可以导入主机资产，也可以下载模板文件，编辑后再导入。



（2） 点击<导出>按钮，可以导出所有主机资产，页面跳转至[文件报表/报表管理 /下载管理]页面。



（3）[文件报表/报表管理 /下载管理]页面新增一条导出记录，待进度条达到 100%转绿后，点击<下载>按钮，即可下载导出的主机资产列表 excel 文件。

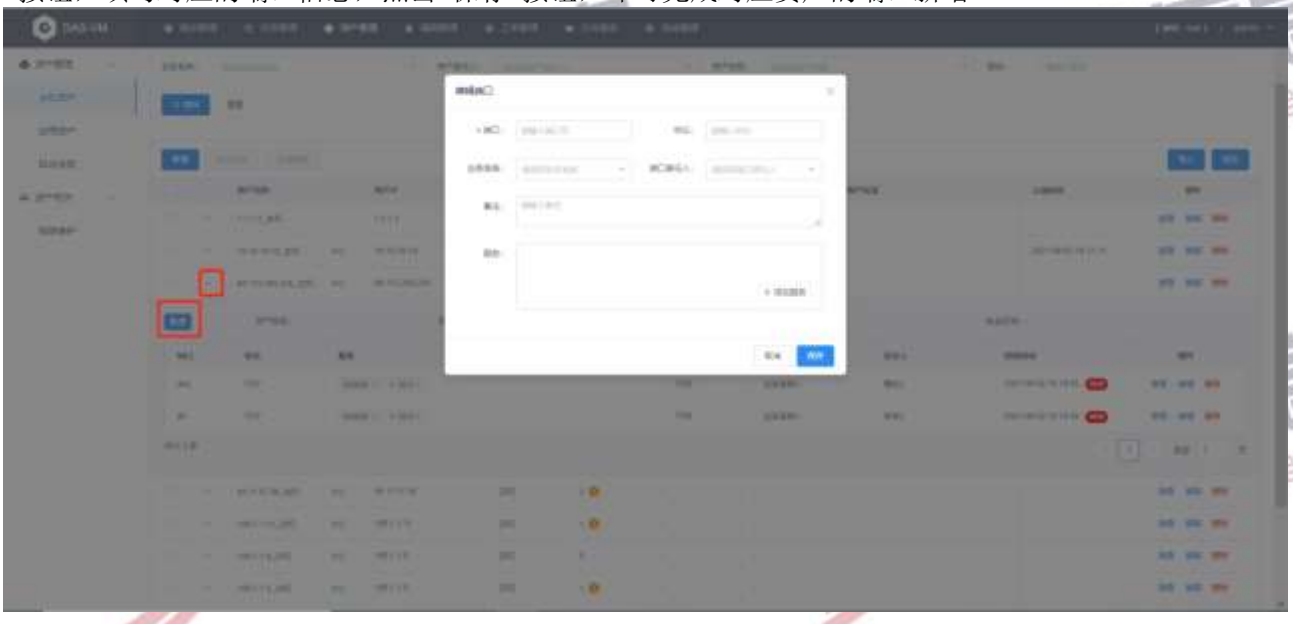


5.1.1.8. 端口管理

（1）新增端口

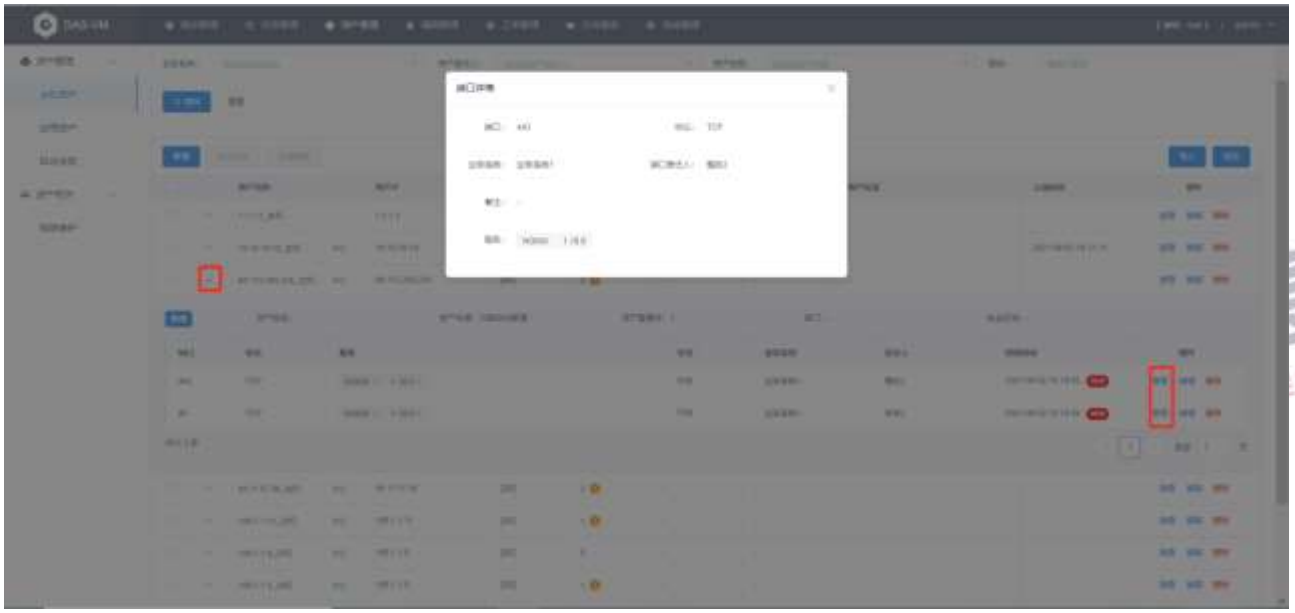
新增或编辑资产时，点击服务信息栏“+”图标，进入新增端口页面，填写对应的端口信息，点击〈保存〉按钮，即可完成对应资产的端口新增。

点击主机资产列表资产名称前面的下拉按钮，展开对应资产下的端口列表，点击端口列表的<新增>按钮，填写对应的端口信息，点击<保存>按钮，即可完成对应资产的端口新增。



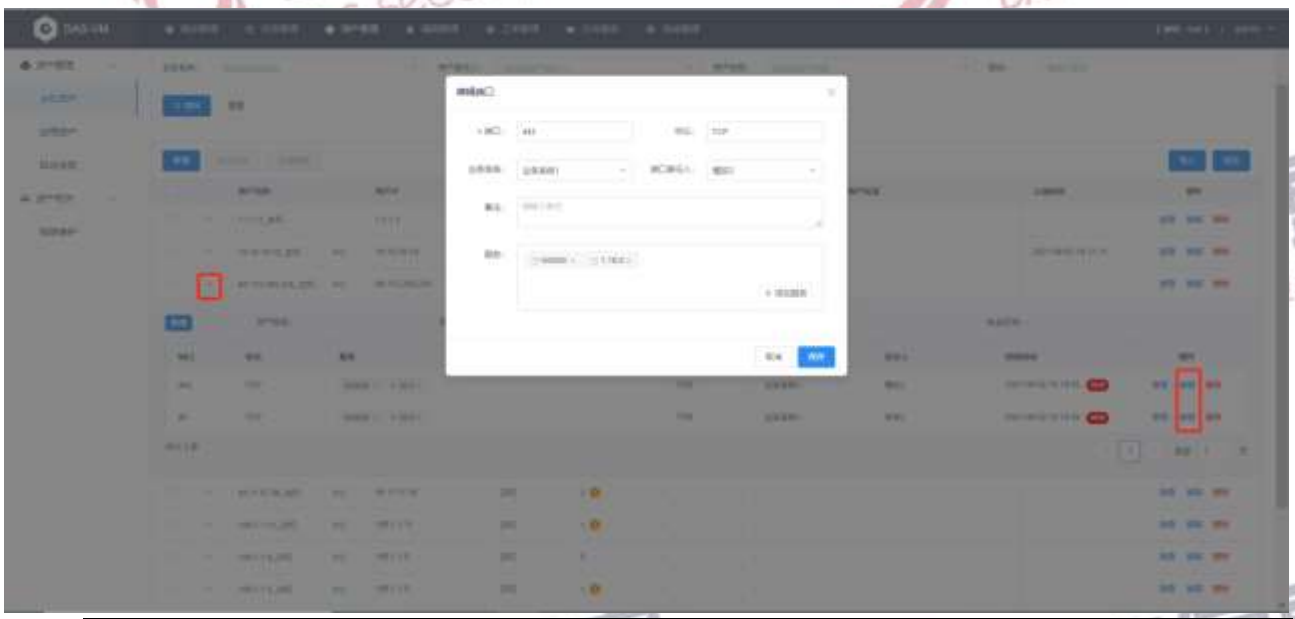
（2）查看端口

点击主机资产列表资产名称前面的下拉按钮，展开对应资产下的端口列表，点击端口列表的<查看>按钮，进入端口详情页面，查看端口信息。或在资产详情页点击服务信息栏端口列表的<查看>按钮，进入端口详情页面，查看端口信息。



（3）编辑端口

点击主机资产列表资产名称前面的下拉按钮，展开对应资产下的端口列表，点击端口列表的<编辑>按钮，进入端口编辑页面，修改端口信息后，单击<保存>按钮，即可完成端口编辑。或在资产详情页点击服务信息栏端口列表的<编辑>按钮，进入端口编辑页面，修改端口信息后，单击<保存>按钮，即可完成端口编辑。

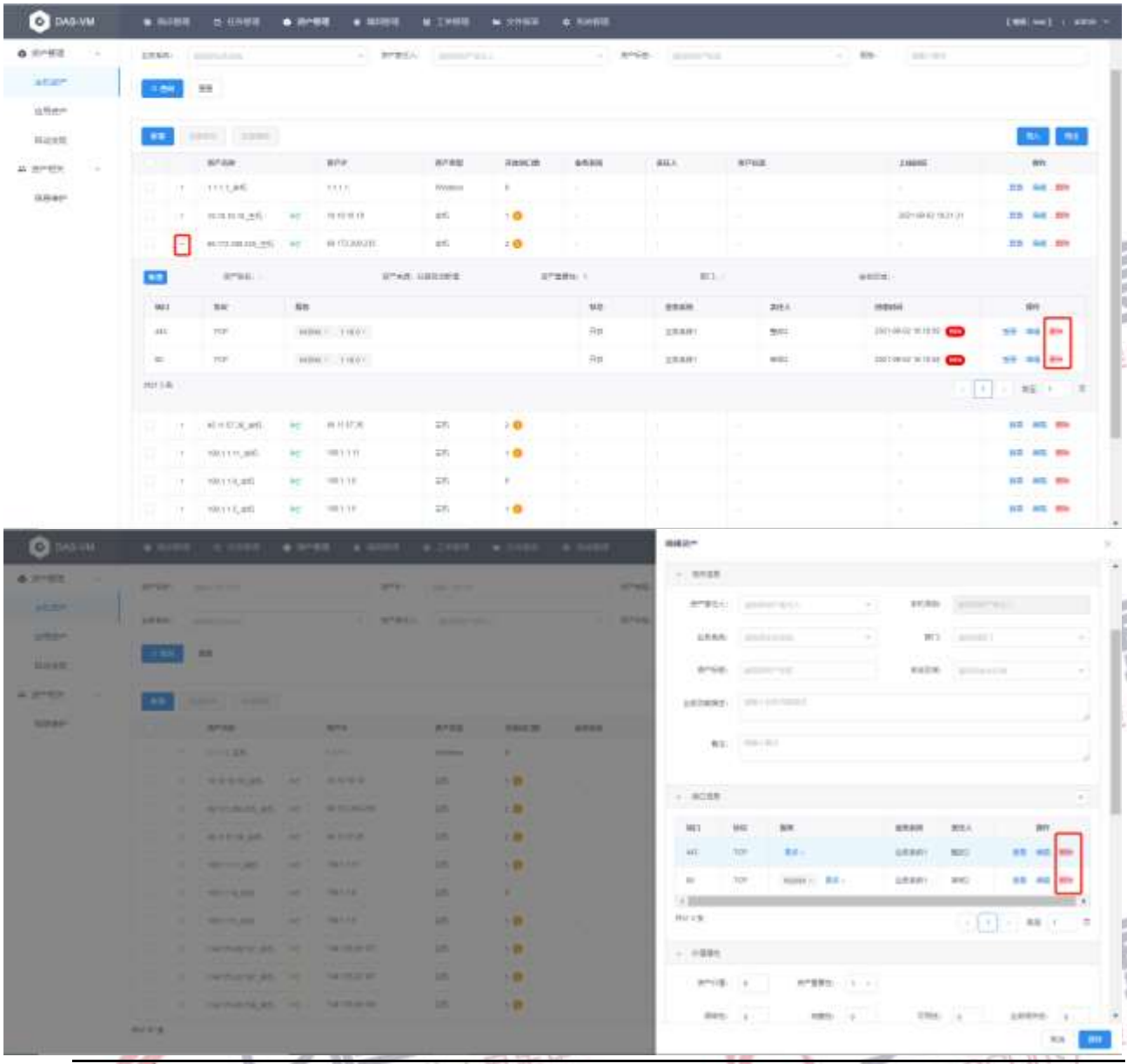


注意

*标记的不能为空。

（4）删除端口

点击主机资产列表资产名称前面的下拉按钮，展开对应资产下的端口列表，点击端口列表的<删除>按钮并确定，可删除对应资产的对应端口信息。或在资产详情页点击服务信息栏端口列表的<删除>按钮，端口删除确认弹窗点击<确定>按钮，即可删除对应资产的对应端口信息。



注意

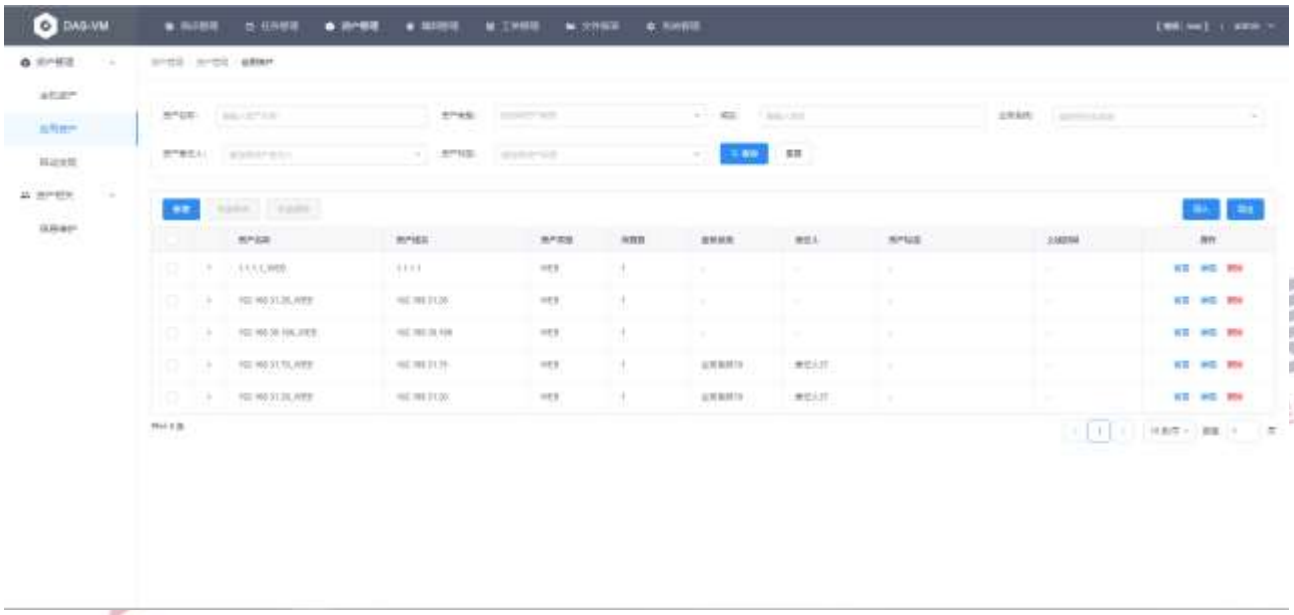
扫描自动发现的端口，只有对业务系统和责任人信息编辑修改后才会出现删除项，并且删除该端口时仅删除该端口的业务系统和责任人信息。

5. 1. 2. 应用资产

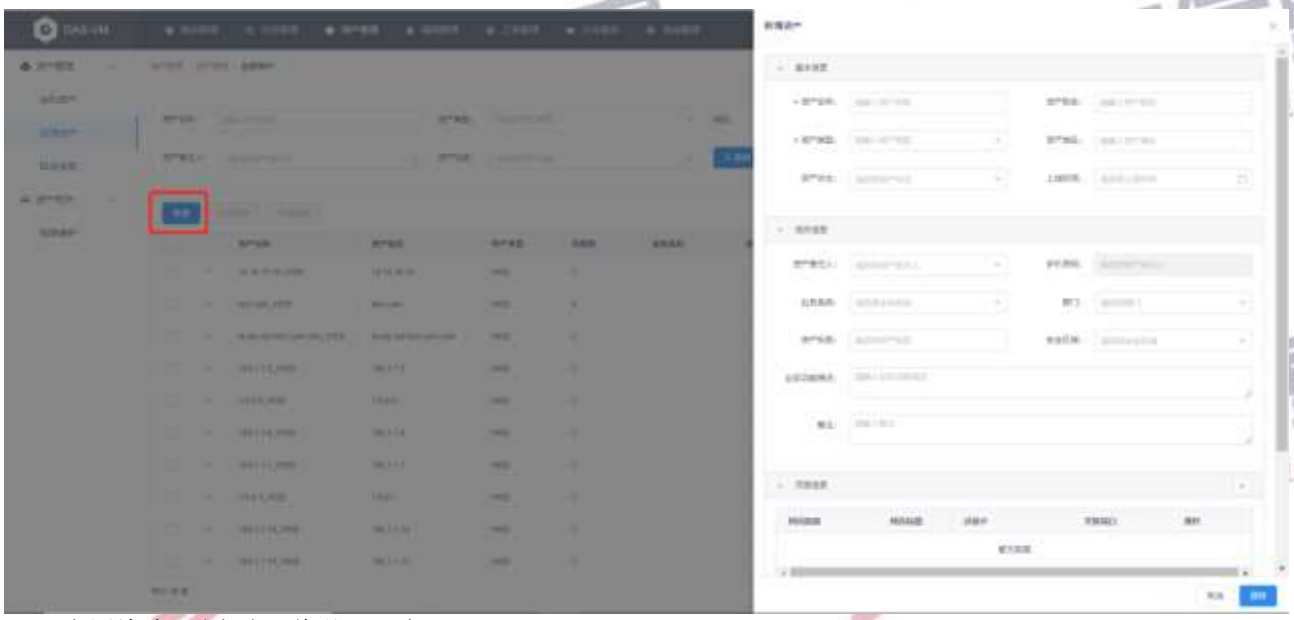
管理所有应用类型资产。

5.1.2.1. 新增资产

（1） 用户 WEB 登录后，进入[资产管理/资产管理/应用资产]页面。



（2） 点击<新增>按钮，进入新增应用资产页面，填写对应的资产信息，点击<保存>按钮，即可完成资产新增。



应用资产配置项及说明见下表：

配置项	说明
资产名称	必填项。资产的名称。
资产别名	选填项。资产的别名。
资产类型	必填项。包括：Android、WEB、IOS、公众号、小程序、H5
资产域名	选填项。填写资产域名。
资产状态	选填项。选择资产状态。

上线时间	选填项。资产的上线时间。
业务系统	选填项。资产所属的业务系统。
资产责任人	选填项。资产的负责人。
手机号码	选填项，置灰。所选择的资产责任人的手机号码。
资产标签	选填项。可选择资产标签分类，输入标签名称快速完成资产标签添加，当无资产标签分类时，快速添加资产标签时默认增加名称为“资产”，其重要性为 1。
部门	选填项。资产的部门。
安全区域	选填项。资产的安全区域。
业务功能描述	选填项。应用资产的业务功能描述。
备注	选填项。应用资产的备注。
资产价值	新增资产的资产价值，资产价值由保密性、完整性、可用性、业务相关性四个属性决定。
资产重要性	必填项。新增资产的重要性，从 1 到 10 划分，1 的重要性最低，10 的重要性最高。
保密性	选填项。新增资产的保密性，取值范围为 0~10，0 的重要性最低，10 的重要性最高，保留一位小数。
完整性	选填项。新增资产的完整性，取值范围为 0~10，0 的重要性最低，10 的重要性最高，保留一位小数。
可用性	选填项。新增资产的可用性，取值范围为 0~10，0 的重要性最低，10 的重要性最高，保留一位小数。
保密性	选填项。新增资产的保密性，取值范围为 0~10，0 的重要性最低，10 的重要性最高，保留一位小数。

注意

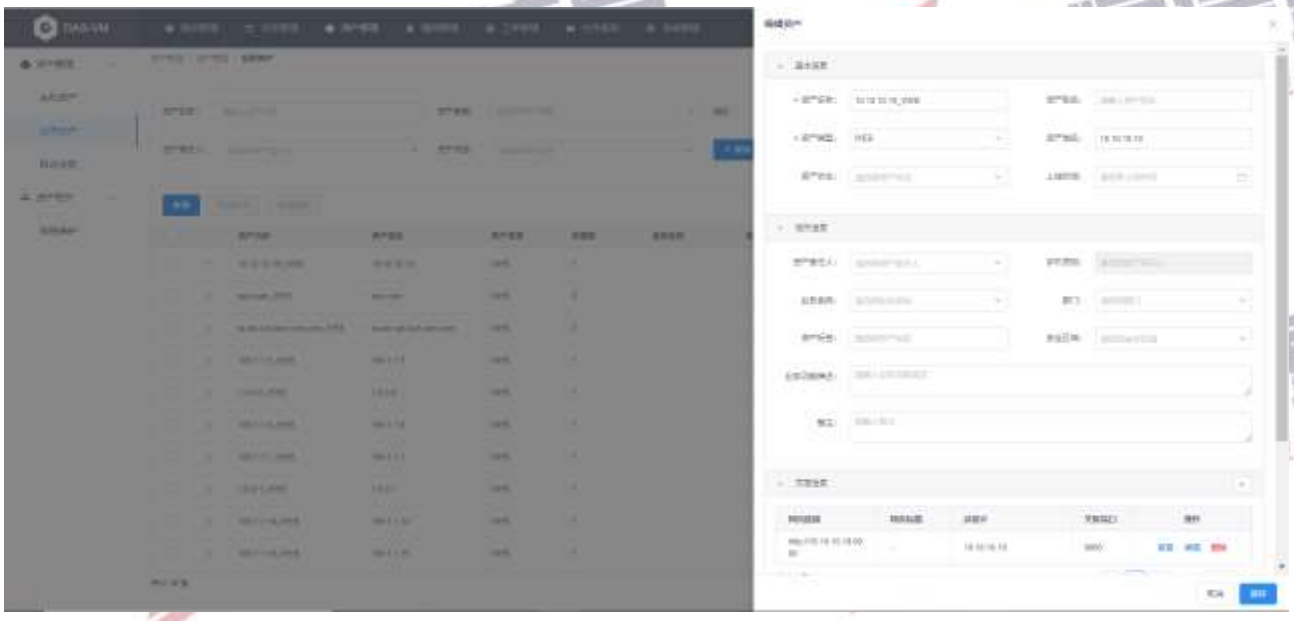
带有“*”号的必须填写，才能成功添加资产。

5.1.2.2. 查看资产

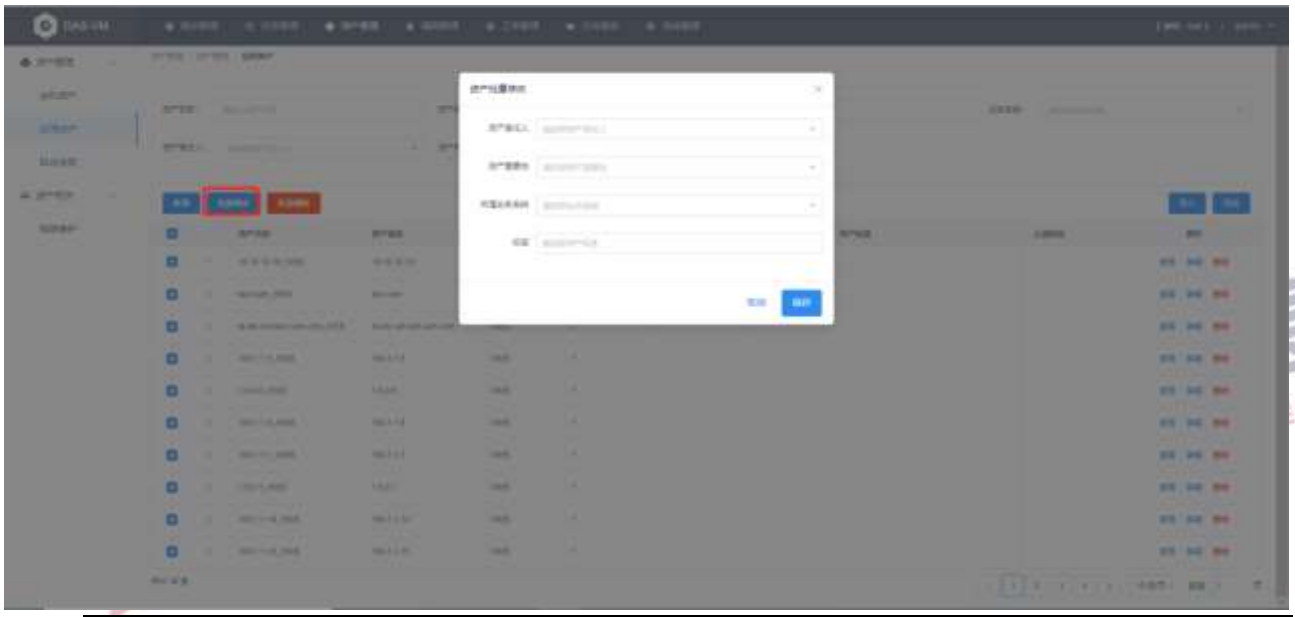
（1） 点击应用资产列表的<查看>按钮，进入资产详情页面，查看资产信息和相关配置信息。

5.1.2.3. 编辑资产

（1） 点击应用资产列表的<编辑>按钮，进入资产编辑页面，修改资产信息后，单击<保存>按钮，即可完成资产编辑。



（2）勾选多个资产后，点击<批量修改>按钮，进入资产批量修改页面，修改资产信息后，单击<保存>按钮，即可完成资产的批量编辑。



注意

批量修改只能修改资产的资产负责人、资产重要性、所属业务系统和资产标签这四项。

5.1.2.4. 删除资产

（1） 点击应用资产列表的<删除>按钮并确定，可删除对应资产的资产信息和相关配置信息。

（2） 勾选多个资产后，点击<批量删除>按钮，资产删除确认弹窗点击<确定>按钮，即可删除勾选的多个资产。

5.1.2.5. 查询资产

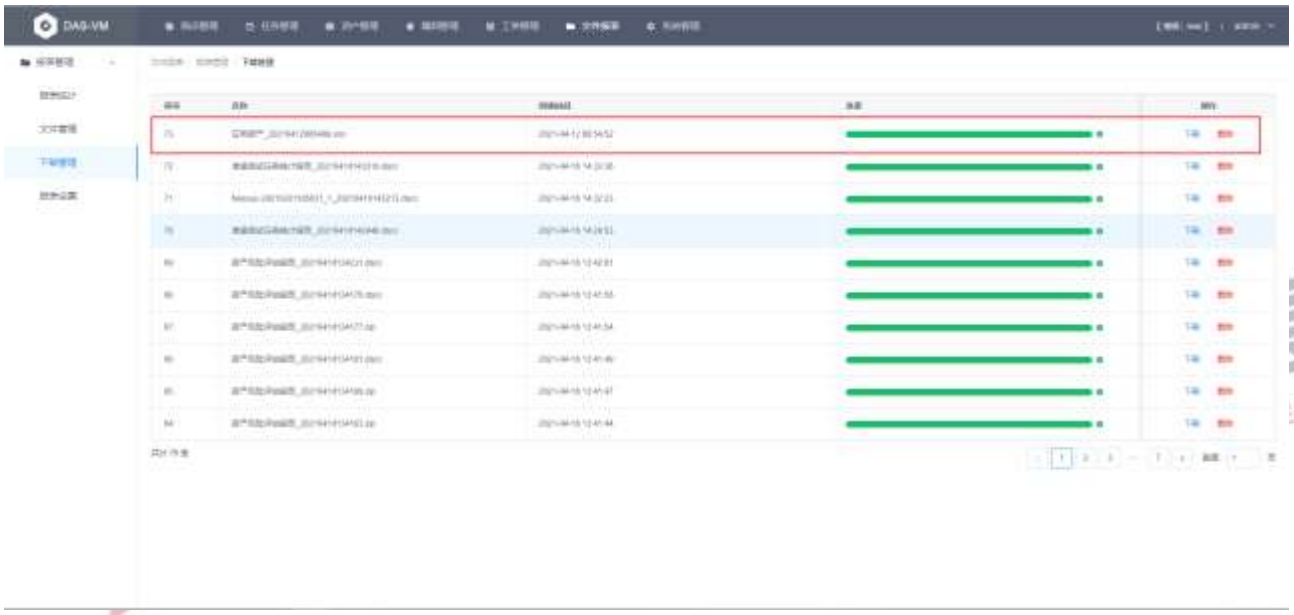
（1） 设置查询条件，可在应用资产列表中进行指定资产查询，条件设置后，点击<查询>按钮，进行查询。点击<重置>按钮，可清空查询条件。

5.1.2.6. 导入导出

（1） 点击<导入>按钮，选择 excel 文件后，点击<上传>按钮可以导入应用资产，也可以下载模板文件，编辑后再导入。

（2） 点击<导出>按钮，可以导出所有应用资产，页面跳转至[文件报表/报表管理 /下载管理]页面。

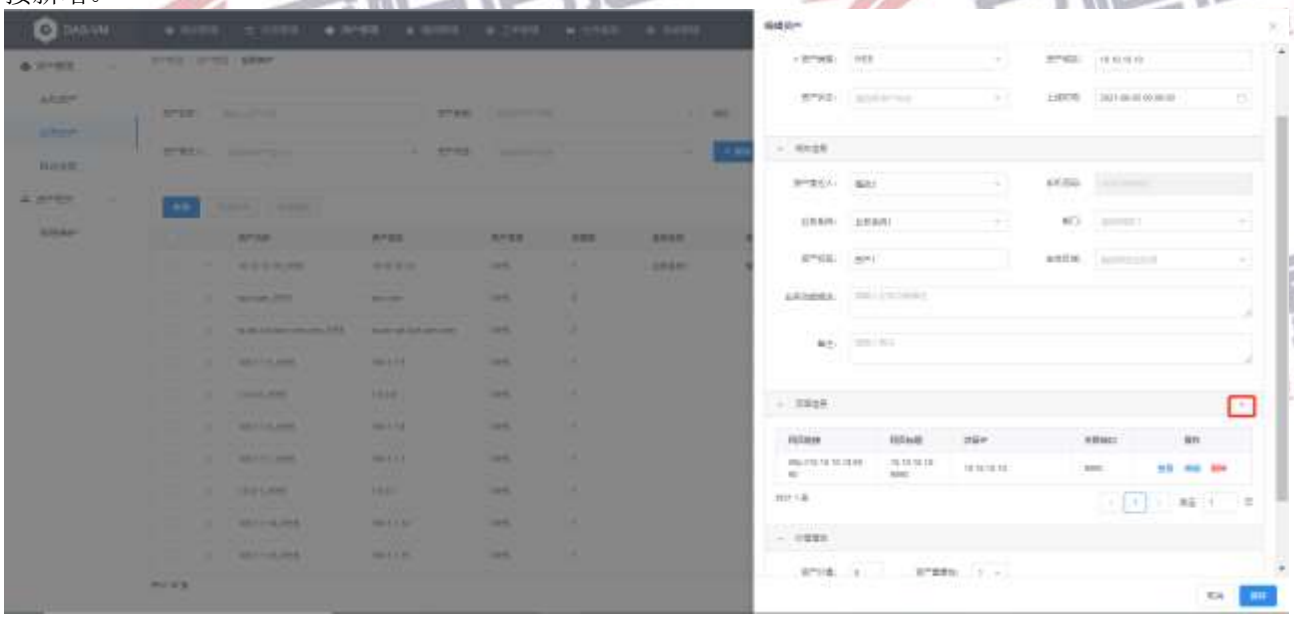
（3） [文件报表/报表管理 /下载管理]页面新增一条导出记录，待进度条达到 100%转绿后，点击<下载>按钮，即可下载导出的主机资产列表 excel 文件。

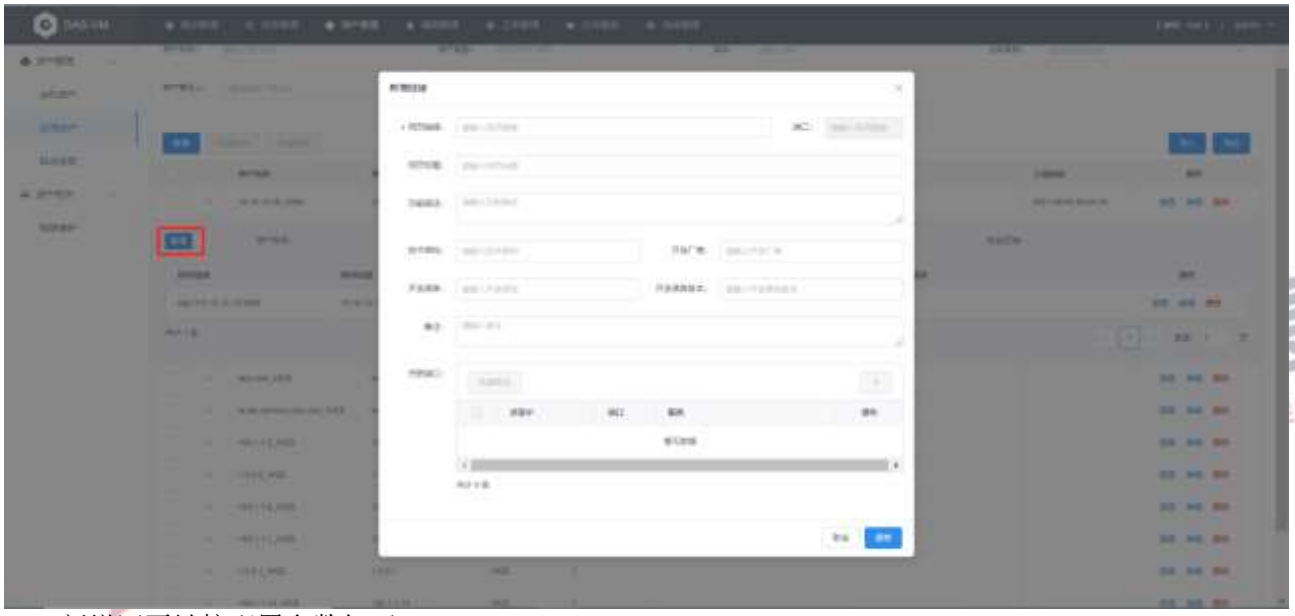


5.1.2.7. 网页链接

（1）新增链接

新增或编辑资产时资产详情页点击网页链接列表“+”图标或应用资产列表下拉展开链接列表点击“新增”按钮，进入新增链接页面，填写对应的链接信息，点击<保存>按钮，即可完成对应资产的链接新增。



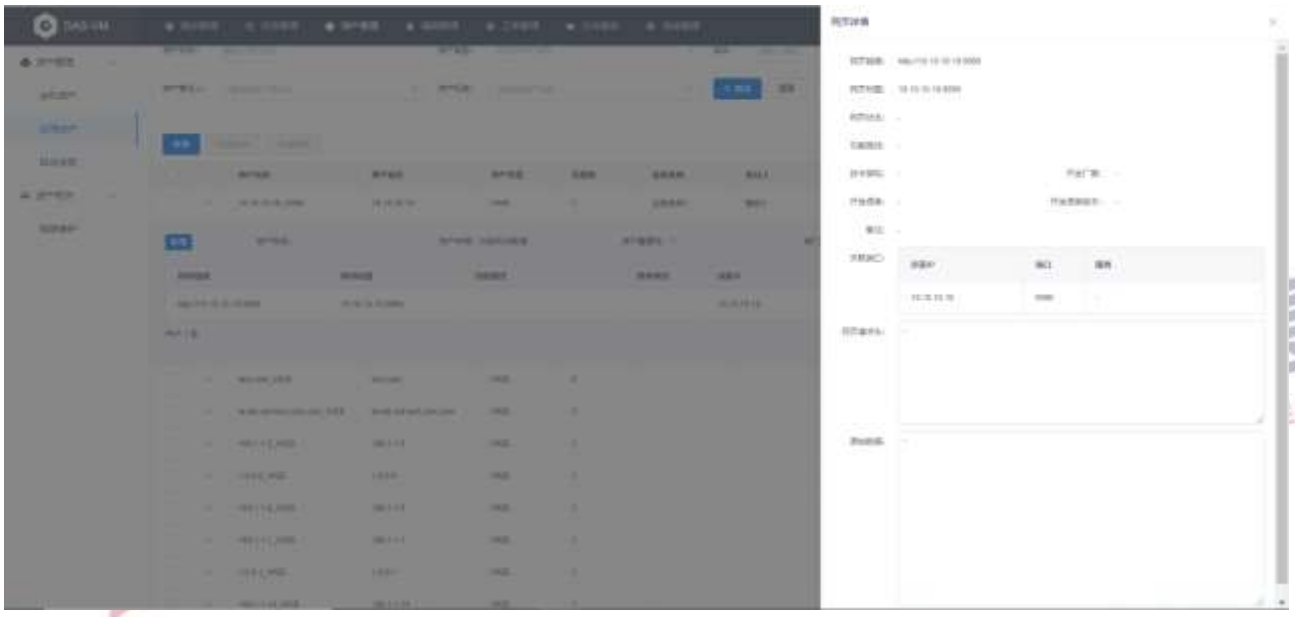


新增网页链接配置参数如下：

配置项	说明
网页链接	必填项。新增网页链接。
端口	依据不同网页链接，自动关联不同端口。
网页标题	选填项。新增网页链接的网页标题。
功能描述	选填项。新增网页链接的功能描述。
技术架构	选填项。新增网页链接的技术架构。
开发厂商	选填项。新增网页链接的开发商。
开发语言	选填项。新增网页链接的开发语言。
开发语言版本	选填项。新增网页链接的开发语言版本。
备注	选填项。新增网页链接的备注。
关联端口	选填项。新增网页链接的关联端口。

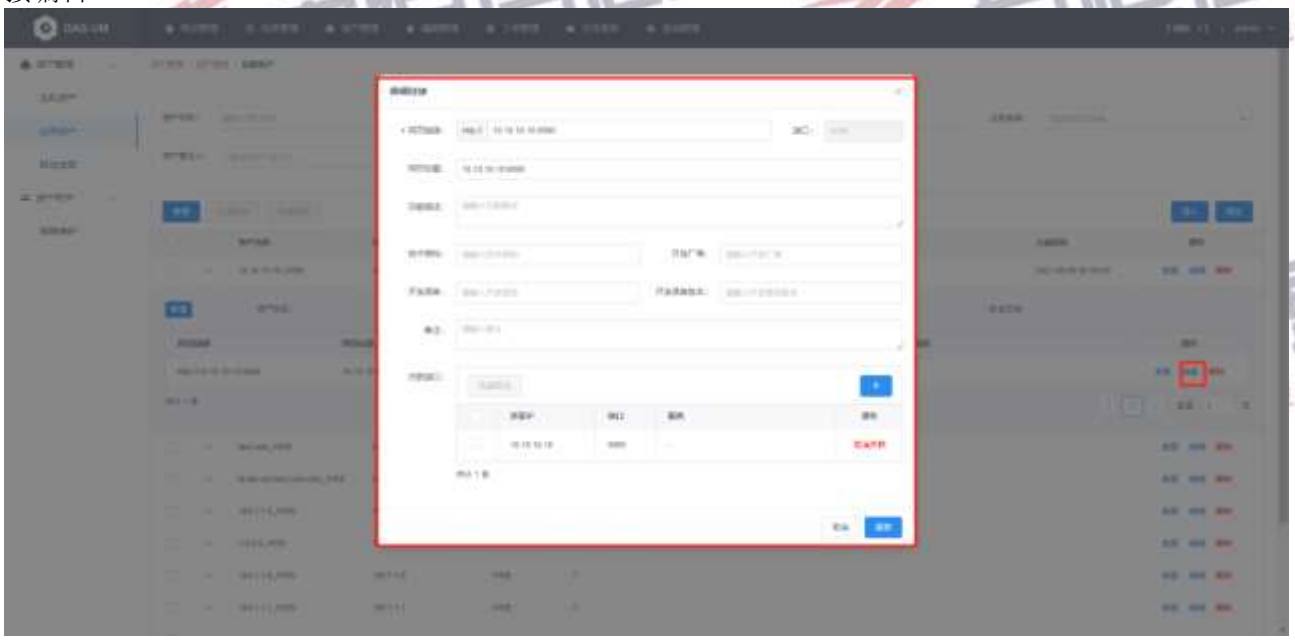
（2） 查看链接

点击应用资产列表资产名称前面的下拉按钮，展开对应资产下的链接列表，点击链接列表的<查看>按钮，进入链接查看页面。或在资产详情页点击链接列表的<查看>按钮，进入链接查看页面。



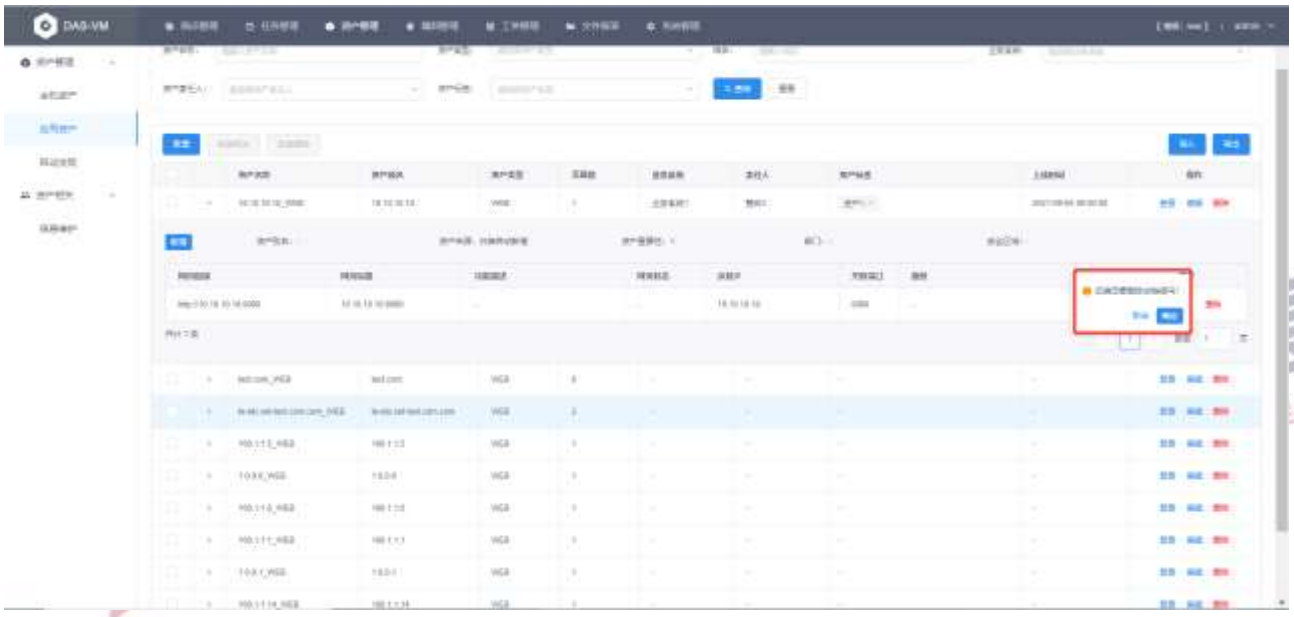
（3） 编辑链接

点击应用资产列表资产名称前面的下拉按钮，展开对应资产下的链接列表，点击链接列表的<编辑>按钮，进入链接编辑页面，修改链接信息后，单击<保存>按钮，即可完成链接编辑。或在资产详情页点击链接列表的<编辑>按钮，进入链接编辑页面，修改链接信息后，单击<保存>按钮，即可完成链接编辑。



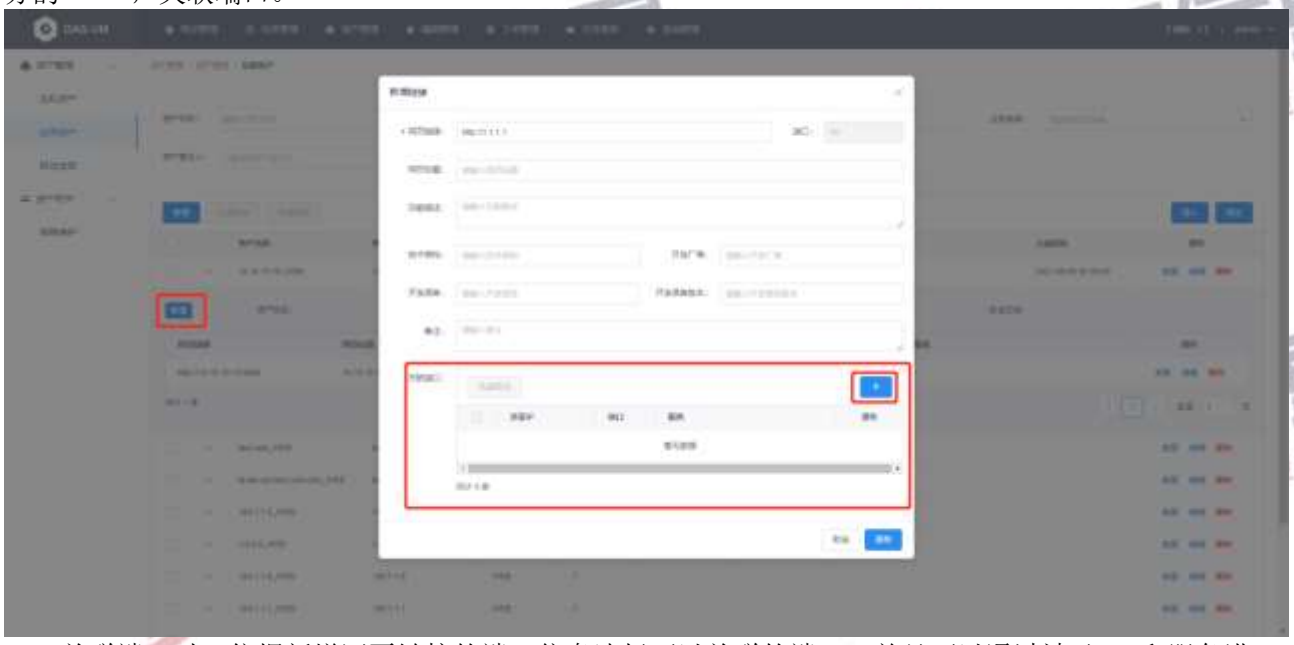
（4）删除链接

点击应用资产列表资产名称前面的下拉按钮，展开对应资产下的链接列表，点击链接列表的<删除>按钮并确定，可删除对应链接。或在资产详情页点击链接列表的<删除>按钮并确定，即可删除链接。

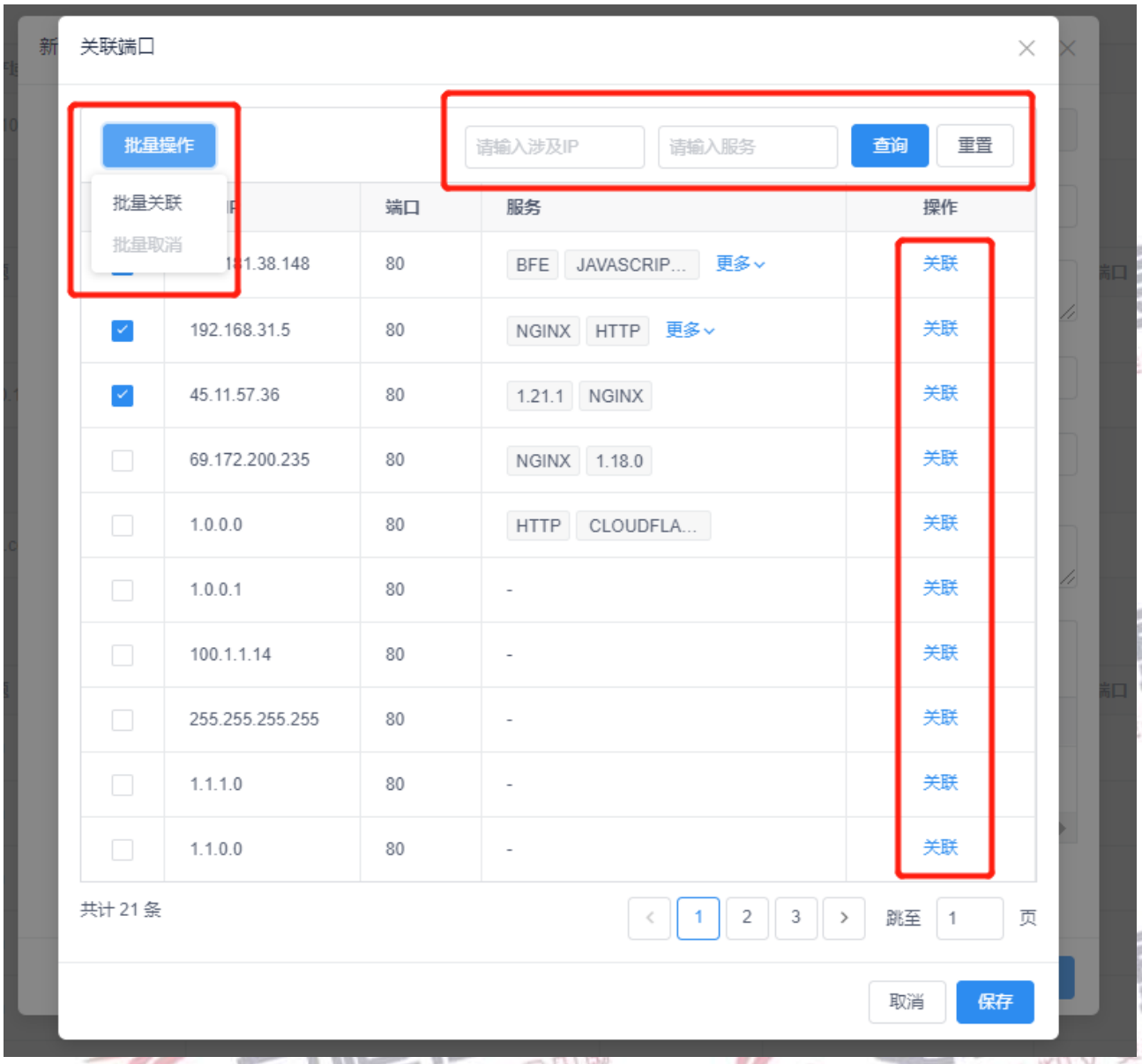


（5）新增关联端口

新增应用资产或者在已有应用资产下新增网页链接时，进入新增网页链接界面，点击关联端口部分的“+”，关联端口。



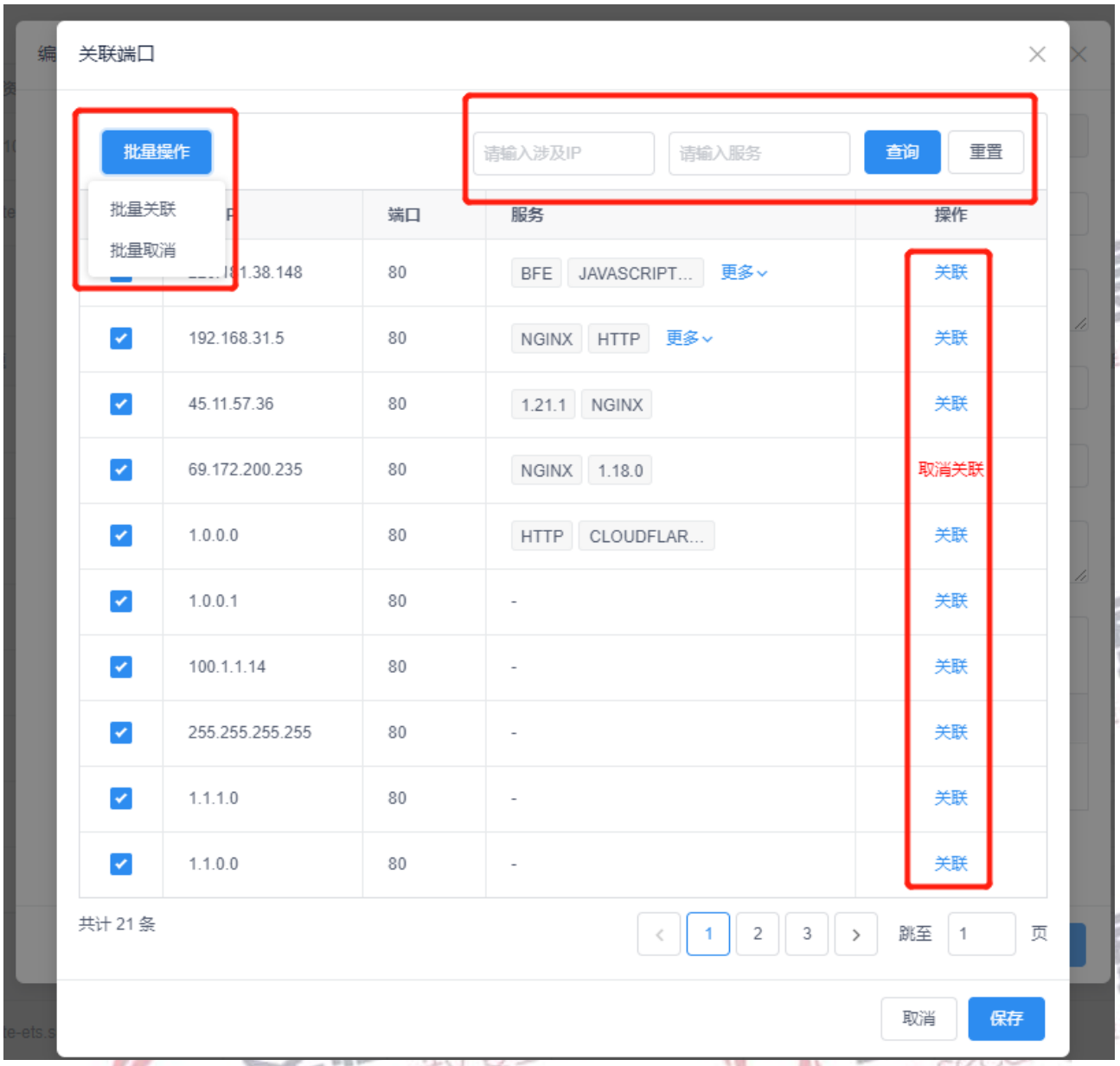
关联端口时，依据新增网页链接的端口信息选择可以关联的端口，并且可以通过涉及 IP 和服务进行查询，勾选相应端口进行批量操作。



（6）编辑关联端口

点击应用资产下拉标，进入编辑网页链接界面，点击关联端口部分的“+”，新增端口。

在关联端口界面，可以通过涉及 IP 和服务查询项查询关联端口信息，然后进行关联或者取消关联，也可以勾选关联端口选项进行批量关联或者取消关联。

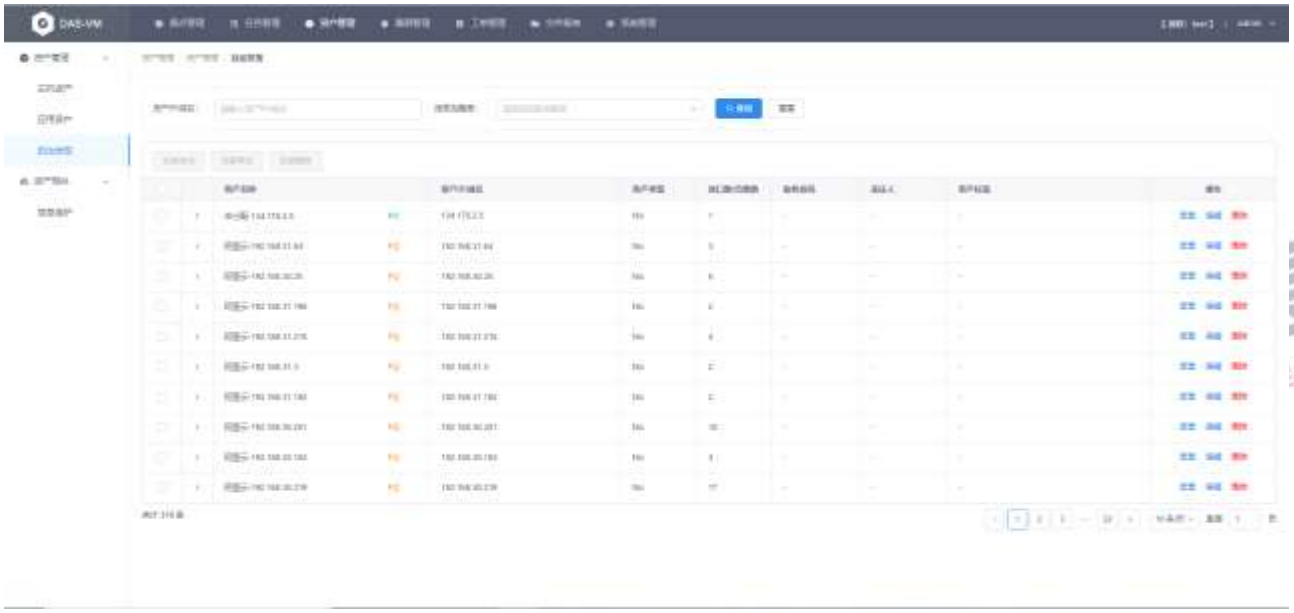


5. 1. 3. 自动发现

平台通过扫描任务完成后自动发现资产，可将发现的资产加入到全部资产列表中。

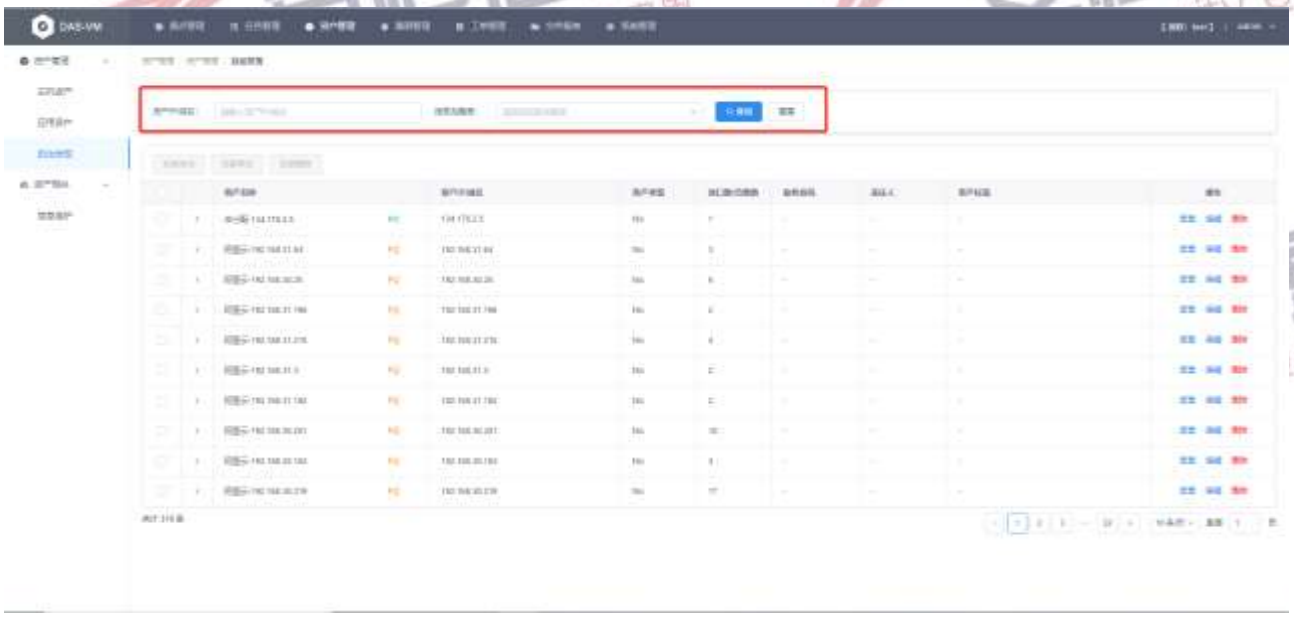
5.1.3.1. 发现资产

（1） 用户 WEB 登录后，进入[资产管理/资产管理/自动发现]页面，显示扫描自动发现的资产。



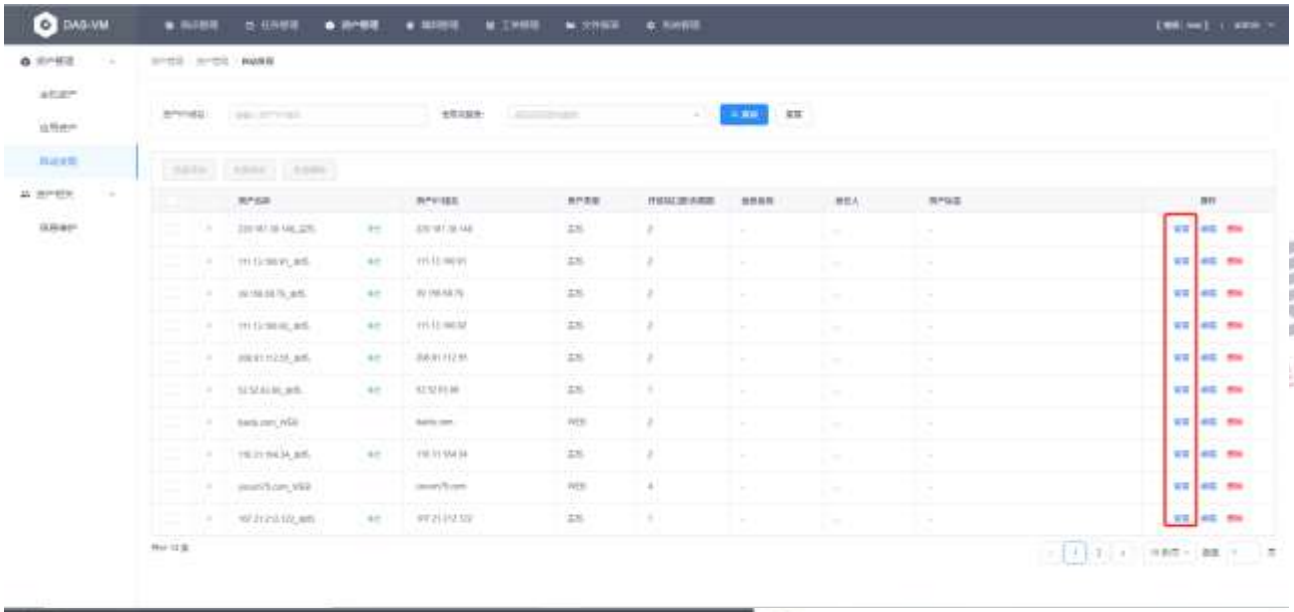
5.1.3.2. 查询资产

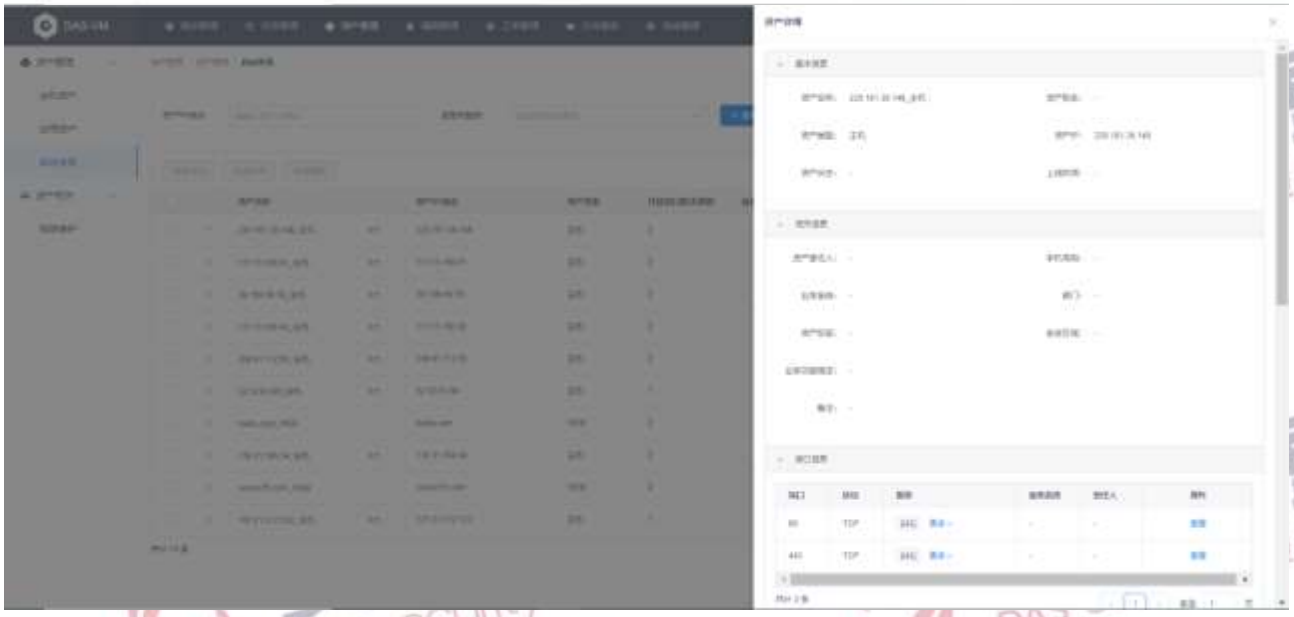
（1） 设置查询条件，可在自动发现列表中进行指定资产查询，条件设置后，点击<查询>按钮，进行查询。点击<重置>按钮，可清空查询条件。



5.1.3.3. 查看资产

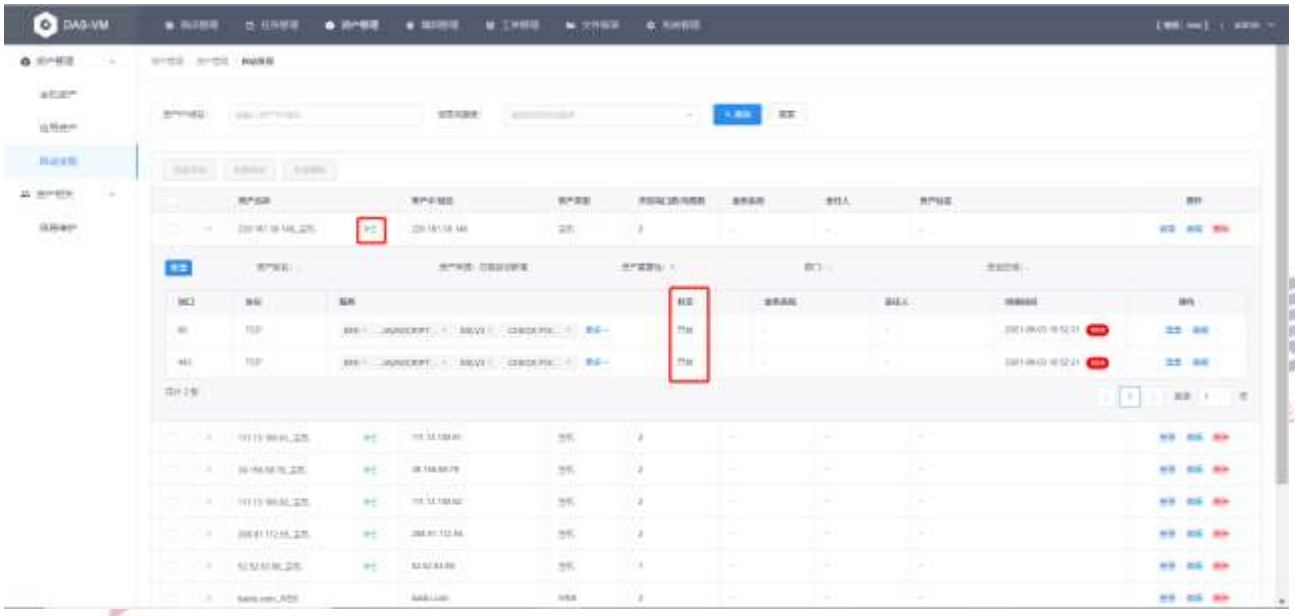
（1） 点击自动发现列表的<查看>按钮，进入资产详情页面，查看资产相关配置信息。



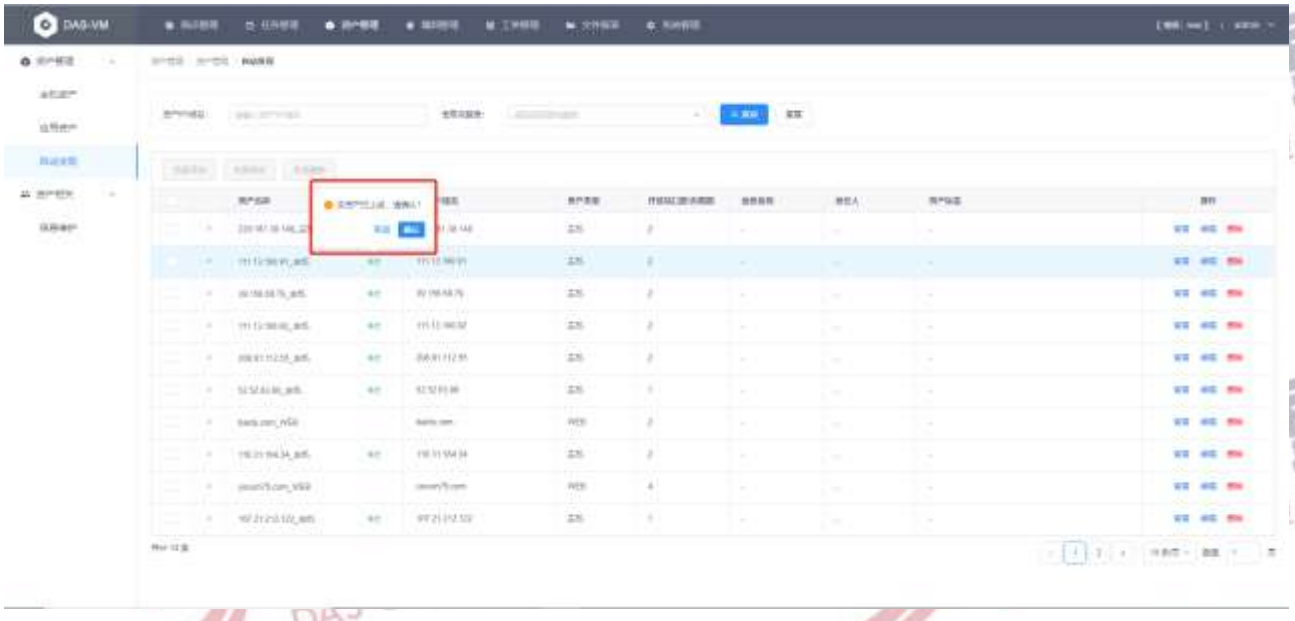


5.1.3.4. 资产上下线告警

（1）资产扫描后，当主机资产存在开放端口时显示上线图标，当主机资产不存在开放端口时显示下线图标。

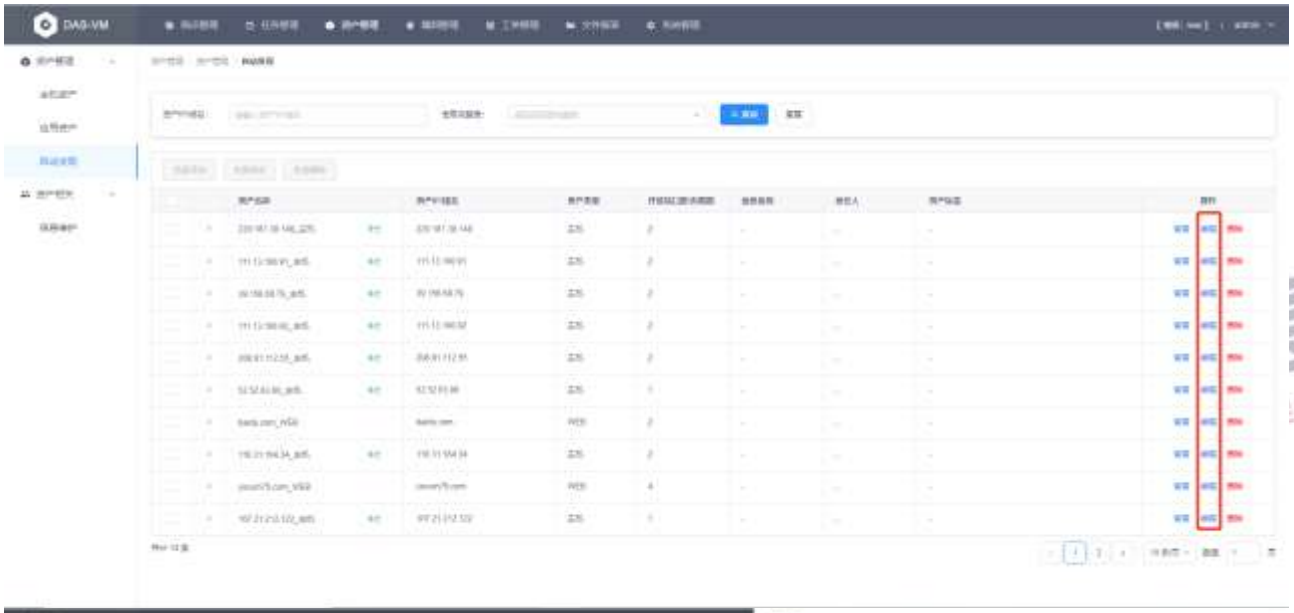


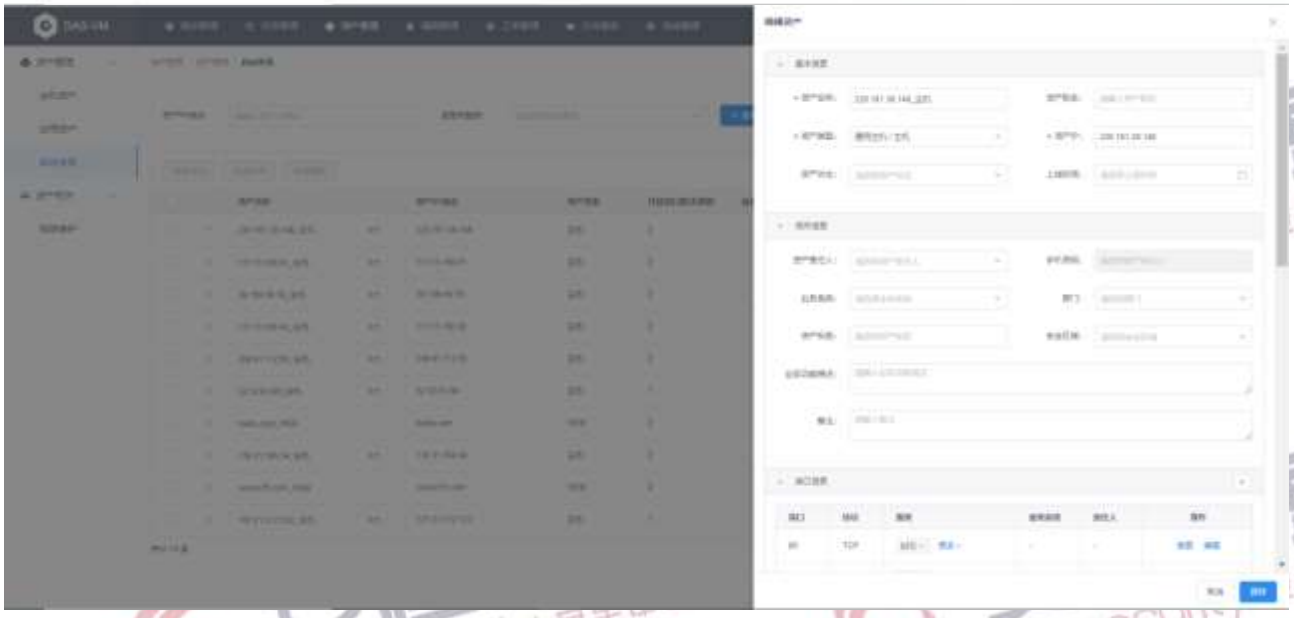
（2）点击上线图标可进行上线确认，确认后对应资产上线时间变更为确认时间。



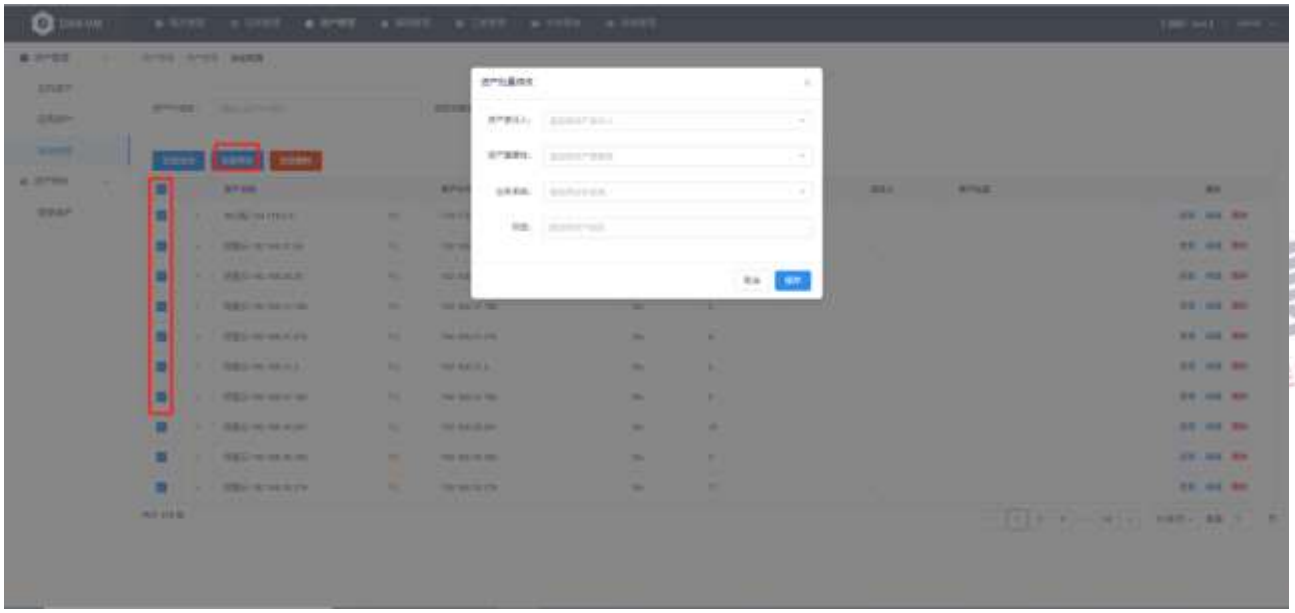
5.1.3.5. 编辑资产

（1） 点击自动发现列表的<编辑>按钮，进入资产编辑页面，修改资产信息后，单击<保存>按钮，即可完成资产编辑。





（2）勾选多个资产后，点击<批量修改>按钮，进入资产批量修改页面，修改资产信息后，单击<保存>按钮，即可完成资产的批量编辑。

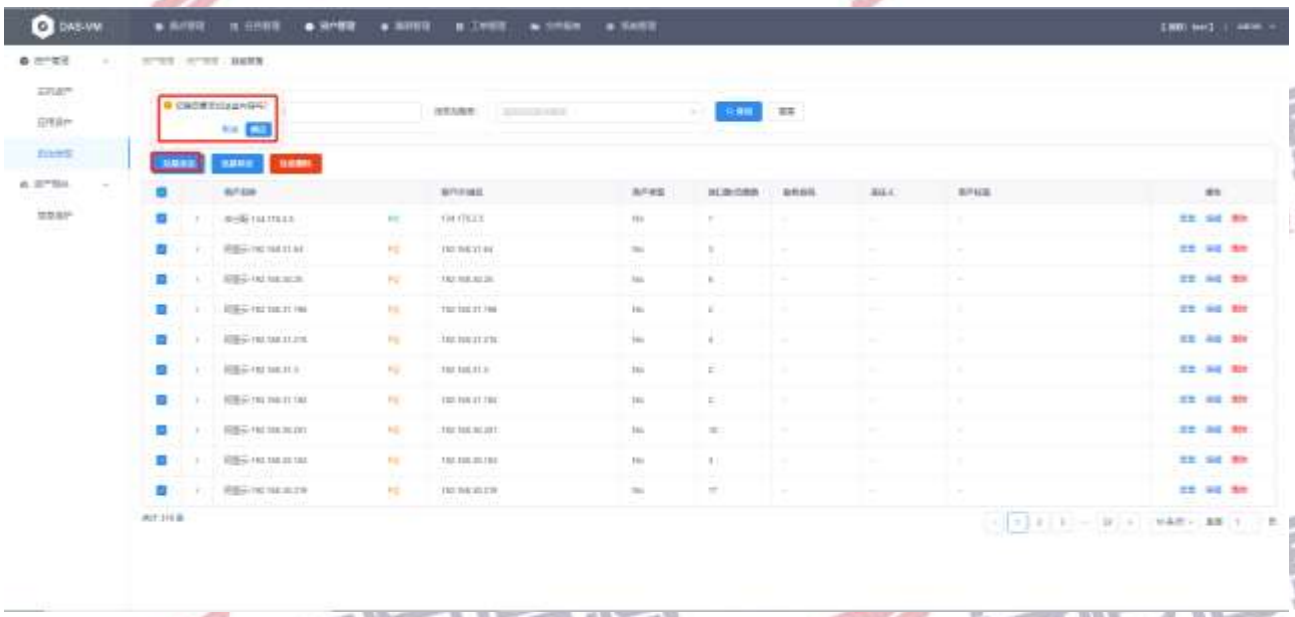


注意

批量修改只能修改资产的资产负责人、资产重要性、所属业务系统和资产标签这四项。

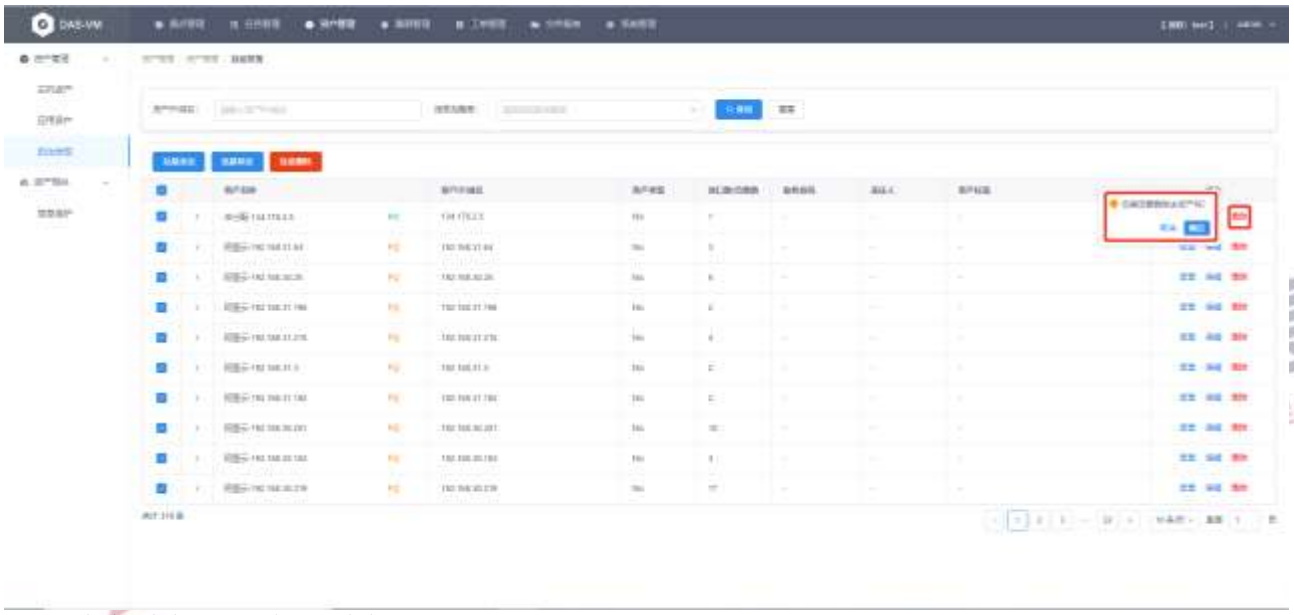
5.1.3.6. 添加资产

（1） 编辑完资产后，自动发现列表勾选需要添加的资产， 点击<批量添加>按钮并确认，即可完成自动发现的资产添加。进入[资产管理/资产管理/主机资产]或[资产管理/资产管理/应用资产]页面，可查看添加的资产。

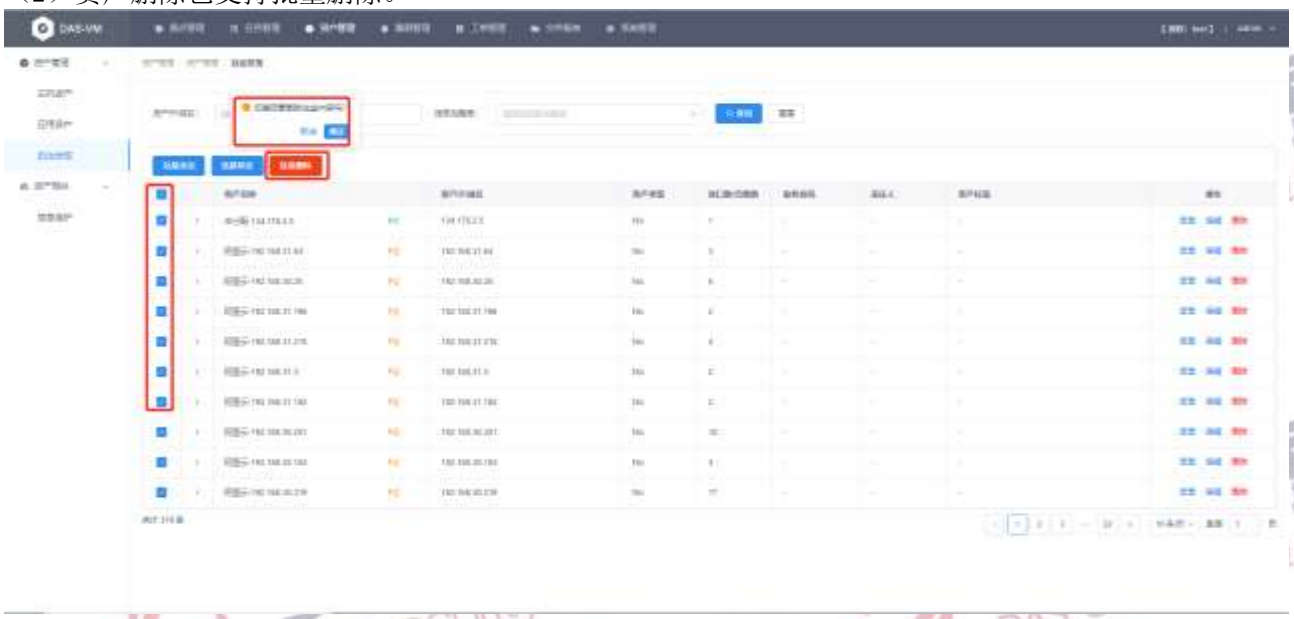


5.1.3.7. 删除资产

（1）点击自动发现列表的<删除>按钮，可以删除资产。



（2）资产删除也支持批量删除。



5.2. 信息维护

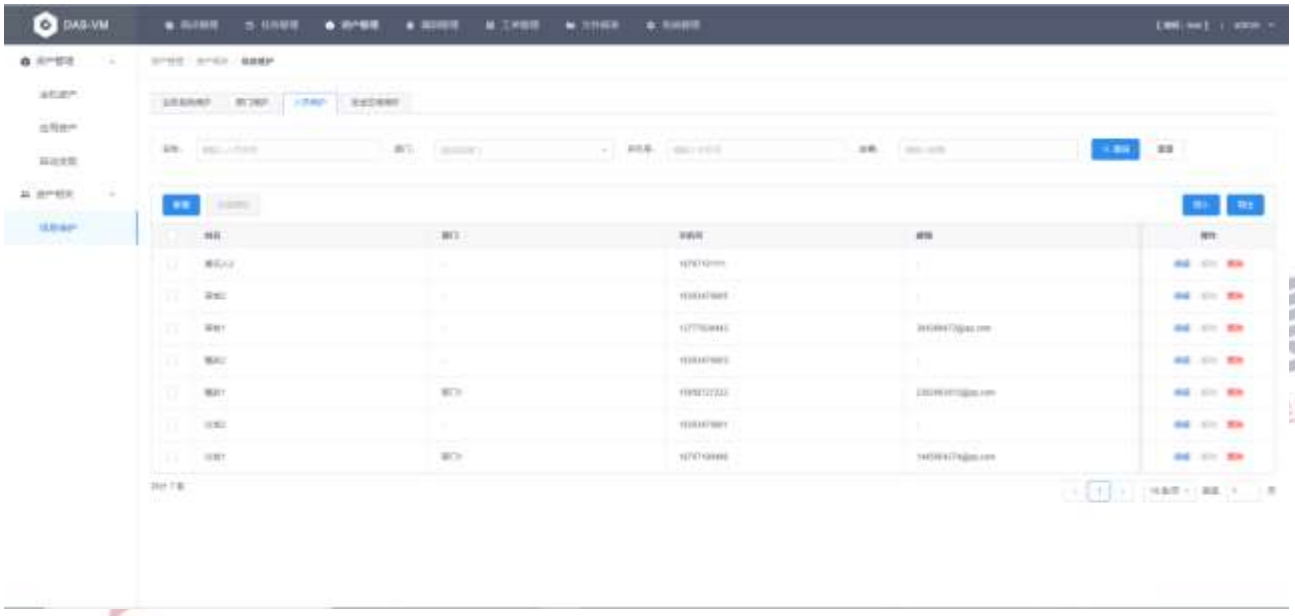
信息维护页面主要用于对人员信息、部门及业务系统等相关信息的维护，包括增、删、改、查、导入、导出等。

5.2.1. 人员维护

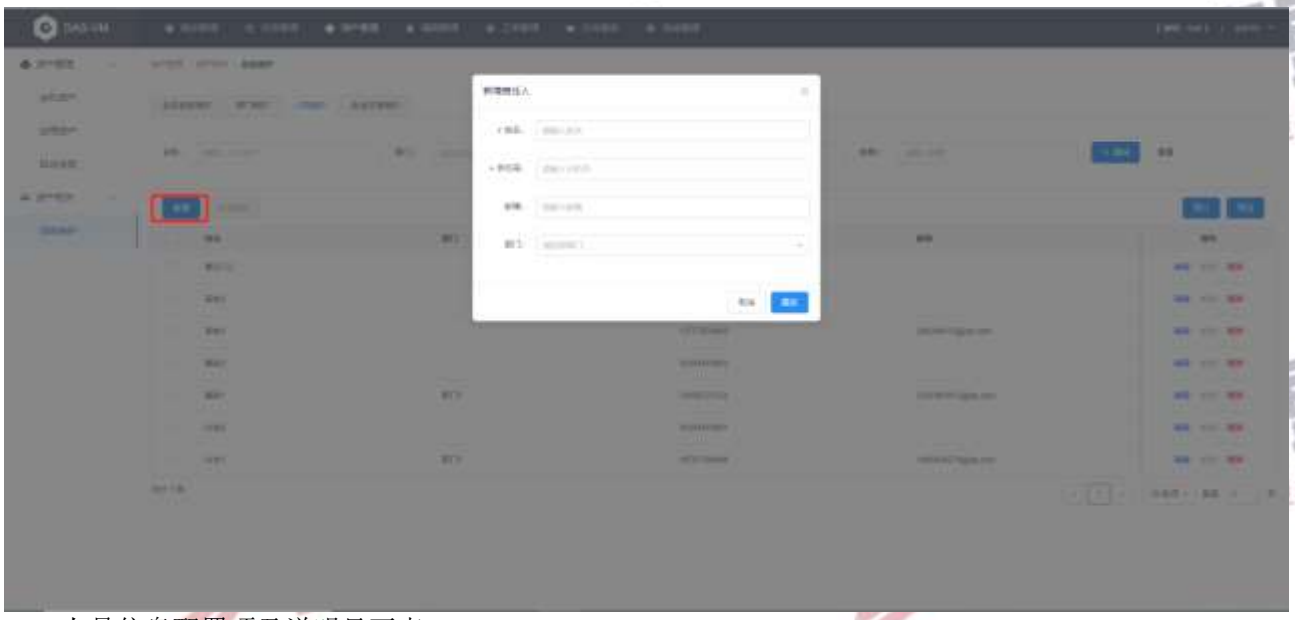
人员维护主要用于对责任人相关信息的增、删、改、查、导入、导出等的管理维护。

5.2.1.1. 新增人员

（1） 用户 WEB 登录后，进入[资产管理/资产相关/信息维护]的人员维护 tab 页。



（2）点击<新增>按钮，弹出新增责任人窗口，填写相应的信息，点击<保存>按钮，即可完成人员添加。

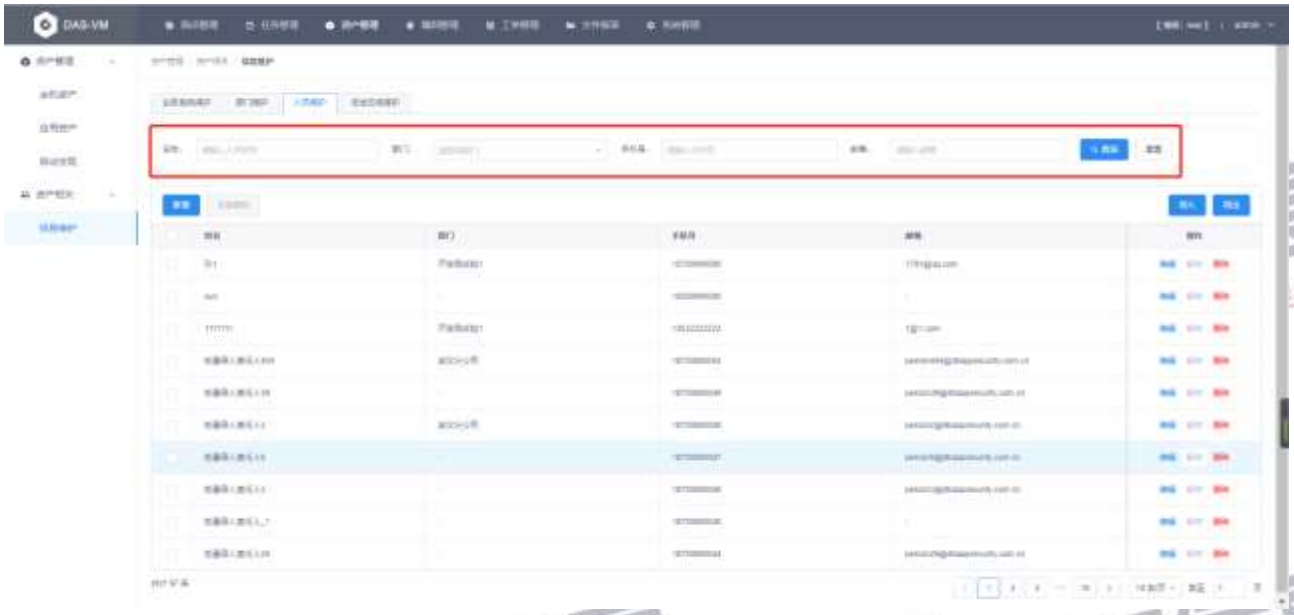


人员信息配置项及说明见下表：

配置项	说明
姓名	必填项。填写责任人姓名。
手机号	必填项。填写责任人手机号。
邮箱	选填项。填写责任人邮箱。
部门	选填项。选择责任人所在的部门。

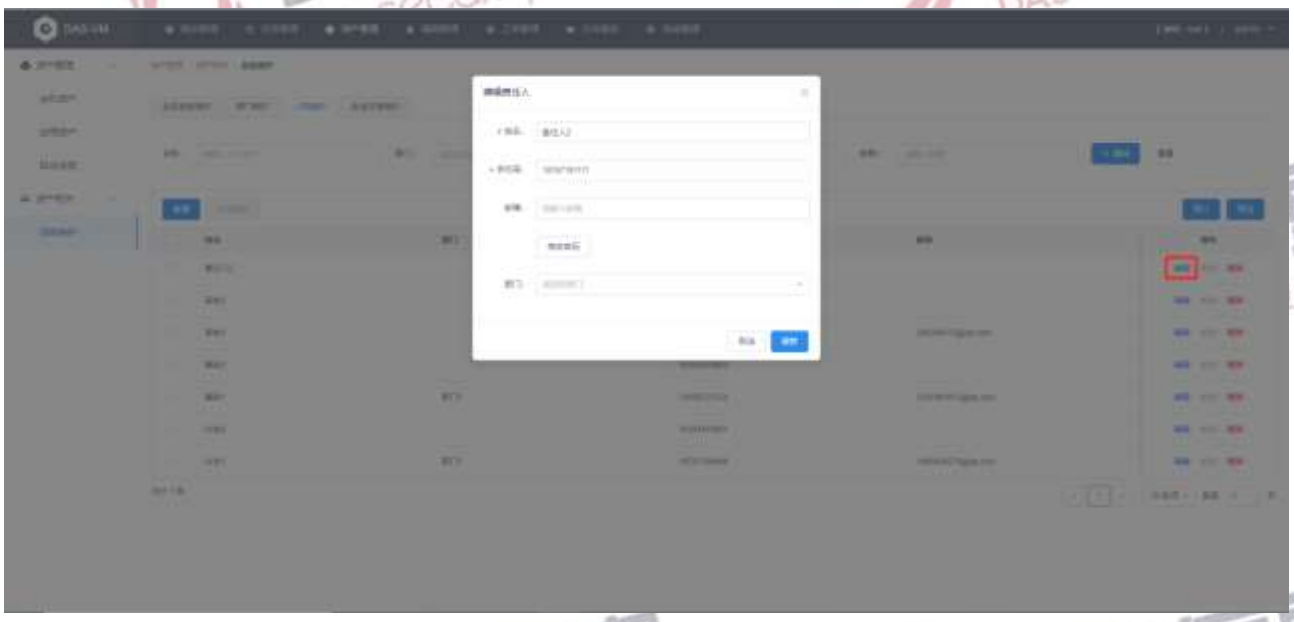
5.2.1.2. 查询人员

（1）设置查询条件，可在人员维护列表中进行指定人员查询，条件设置后，点击<查询>按钮，进行查询。点击<重置>按钮，可清空查询条件。



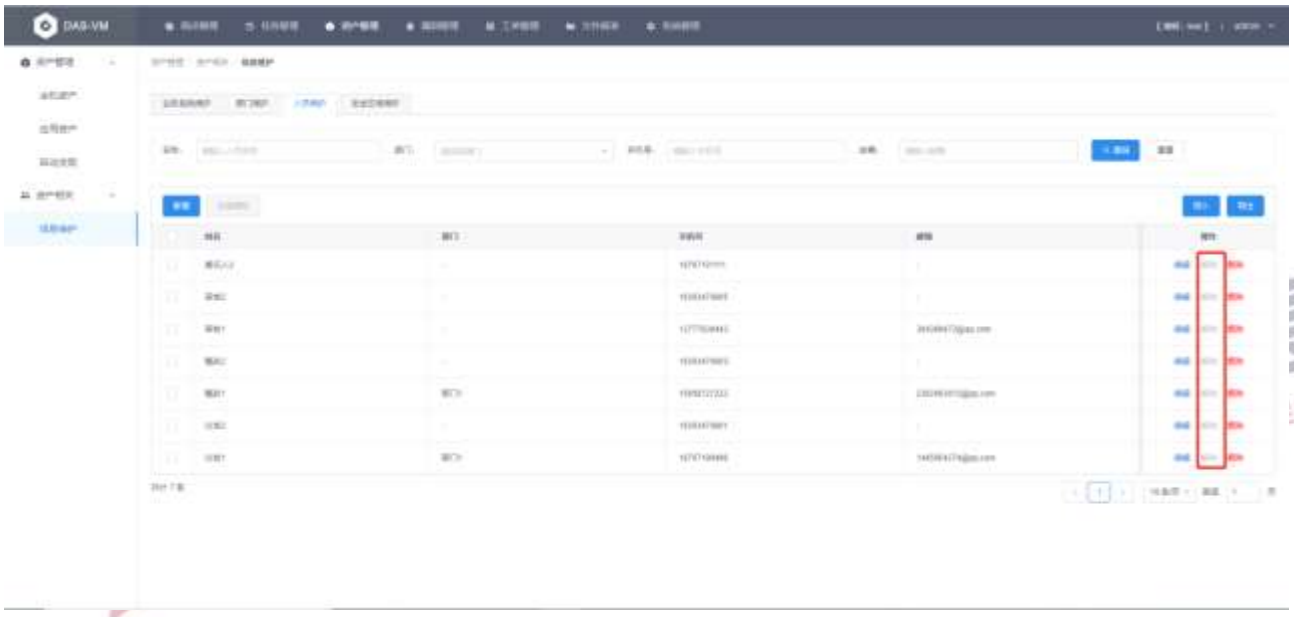
5.2.1.3. 编辑人员

（1） 点击人员列表中的<编辑>按钮，弹出编辑责任人窗口，编辑相应的配置项信息，点击<保存>按钮，即可完成人员信息修改。除此之外，本界面可以修改责任人的密码。



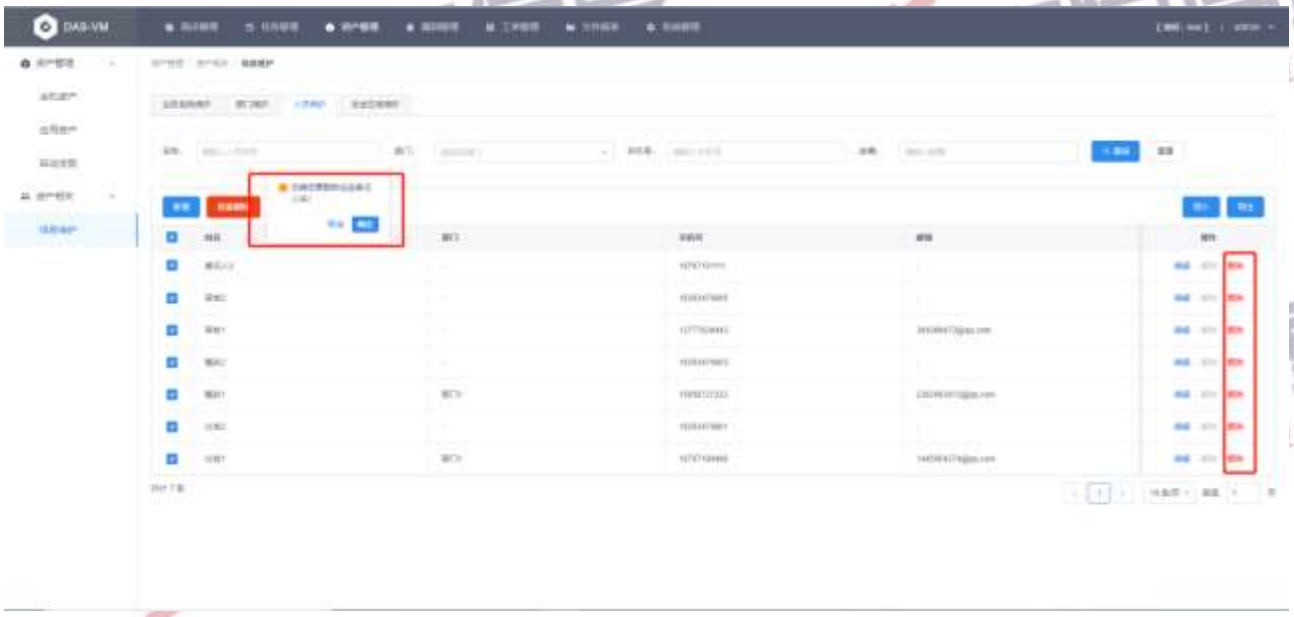
5. 2. 1. 4. 解锁人员

(1)当用户在规定时间内，多次连续登录失败，超过登录安全设置，用户会被锁定，解锁按钮变红。而用户解锁功能，可对超出登录限制已锁定的用户进行解锁，解锁后用户可正常登录。



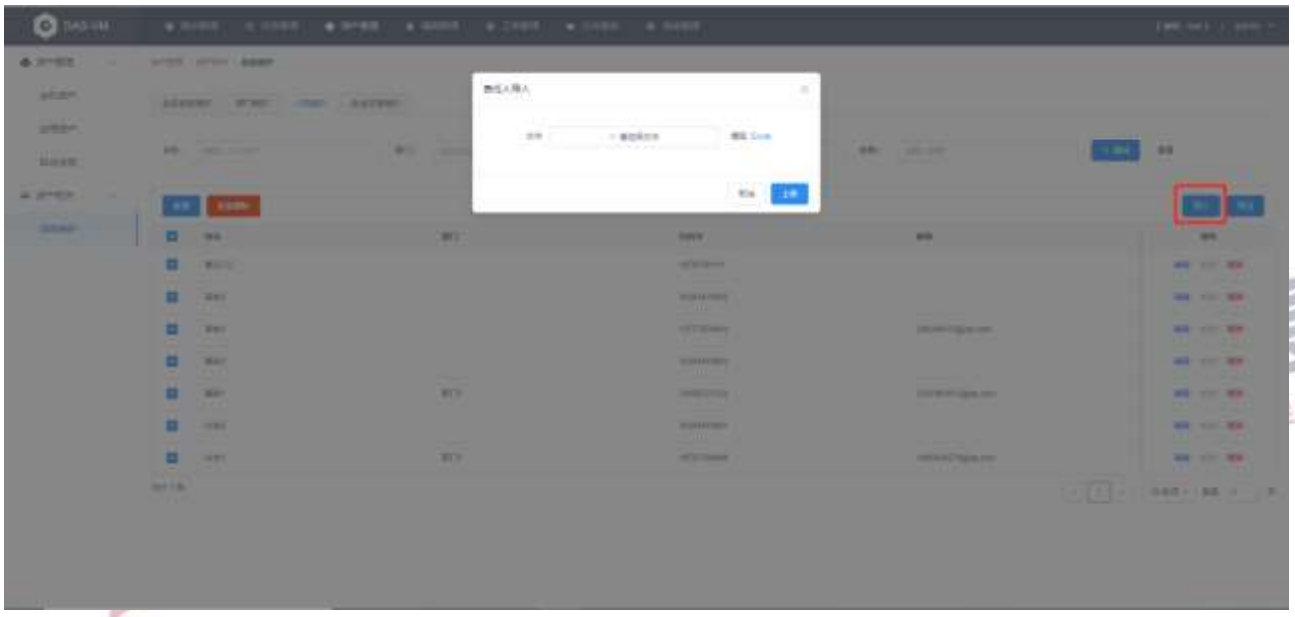
5.2.1.5. 删除人员

（1） 点击人员列表中的<删除>按钮并确定，即可删除对应人员。或者勾选多个人员后，点击人员列表上面的<批量删除>按钮并确定，即可批量删除选中的人员。

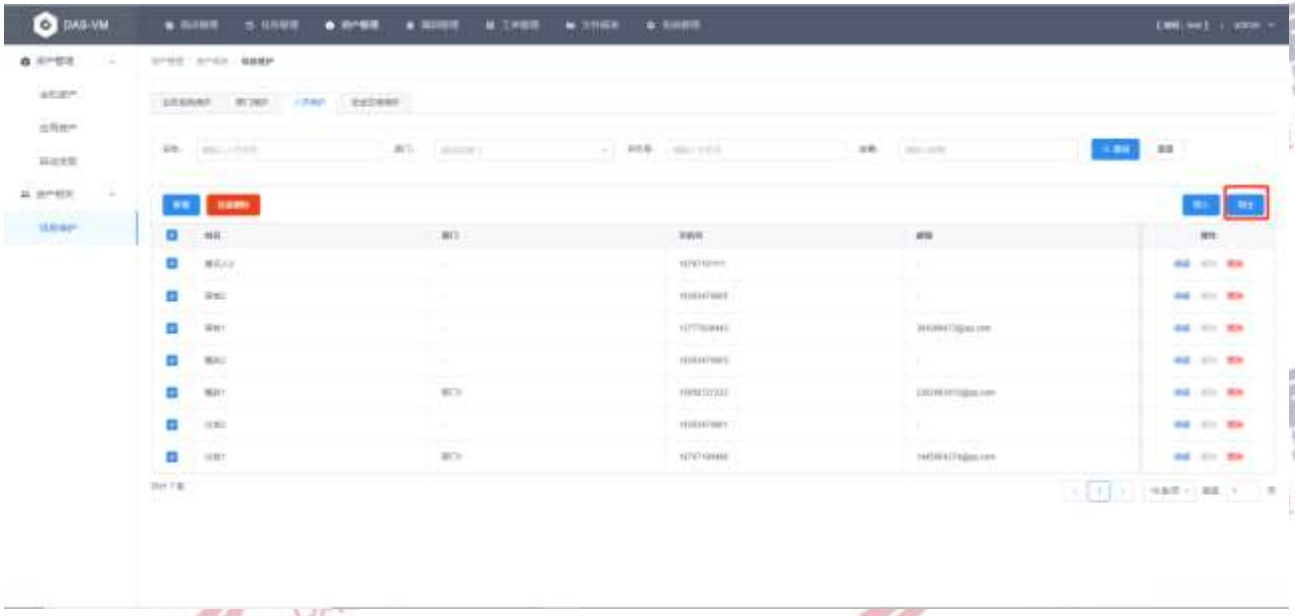


5.2.1.6. 导入导出

（1） 点击<导入>按钮，选择 excel 文件后，点击<上传>按钮可以导入人员，也可以下载模板文件，编辑后再导入。



（2） 点击<导出>按钮，可以导出所有人员，页面跳转至[文件报表/报表管理 /下载管理]页面，待进度条达到 100%转绿后，点击<下载>按钮，即可下载导出的人员列表 excel 文件。



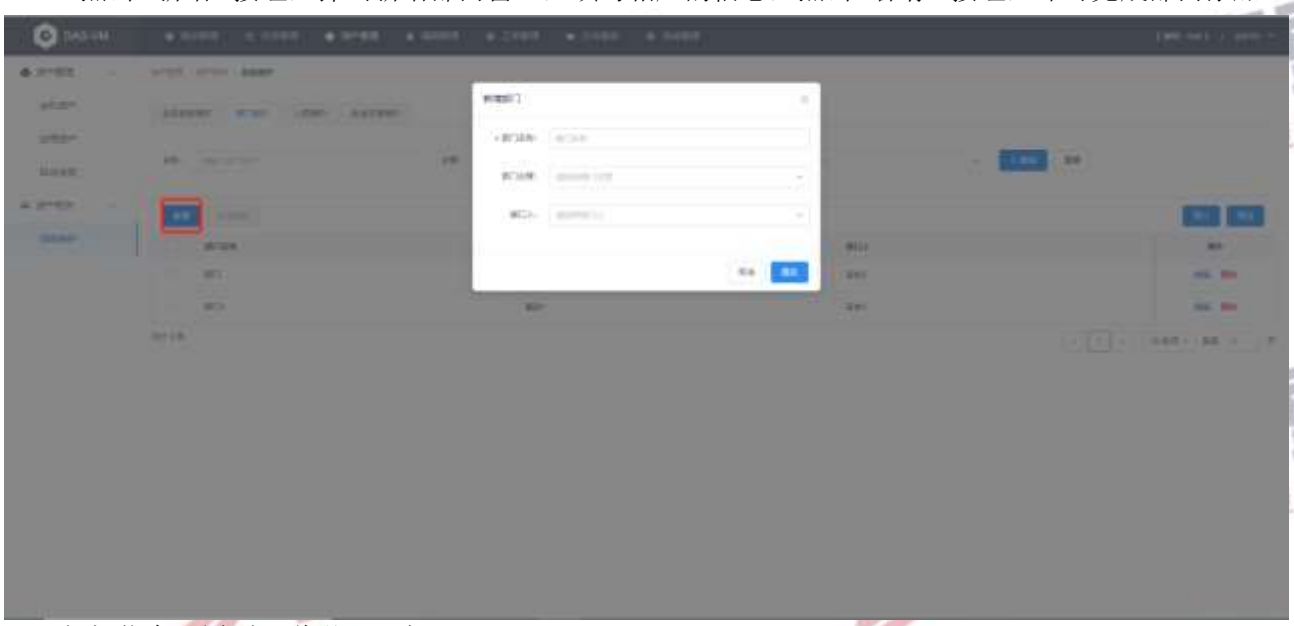
5. 2. 2. 部门维护

部门维护主要用于对部门相关信息的增、删、改、查、导入、导出等的管理维护。

5.2.2.1. 新增部门

（1） 用户 WEB 登录后，进入[资产管理/资产相关/信息维护]的部门维护 tab 页。

（2）点击<新增>按钮，弹出新增部门窗口，填写相应的信息，点击<保存>按钮，即可完成部门添加。

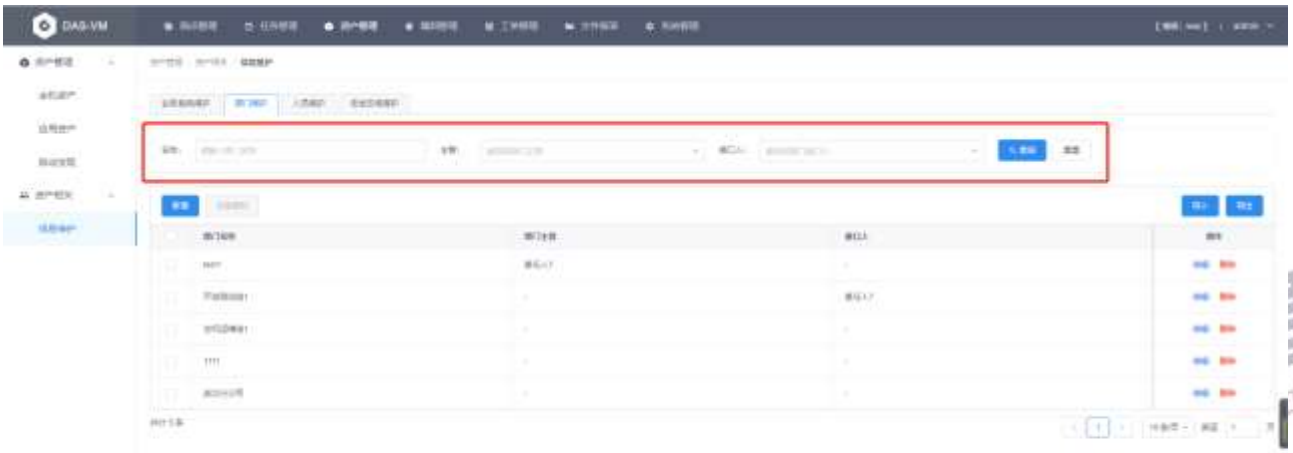


部门信息配置项及说明见下表：

配置项	说明
部门名称	必填项。填写部门名称
部门主管	选填项。选择部门的主管
接口人	选填项。选择部门的接口人

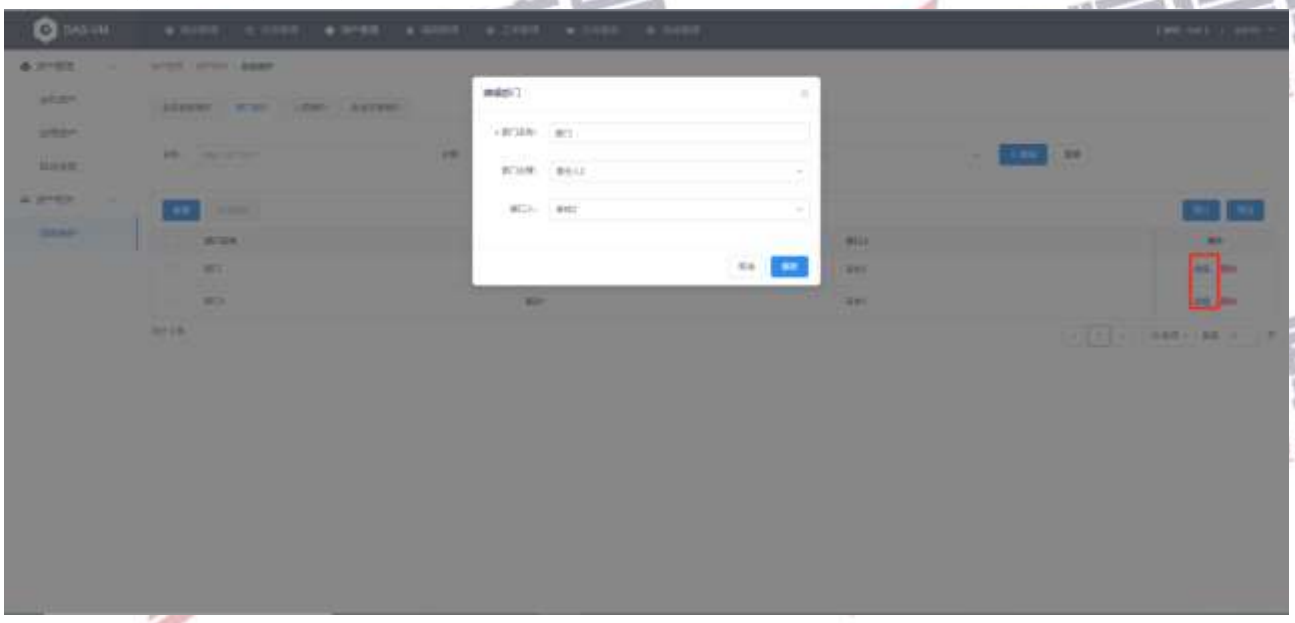
5.2.2.2. 查询部门

（1）设置查询条件，可在部门维护列表中进行指定部门查询，条件设置后，点击<查询>按钮，进行查询。点击<重置>按钮，可清空查询条件。



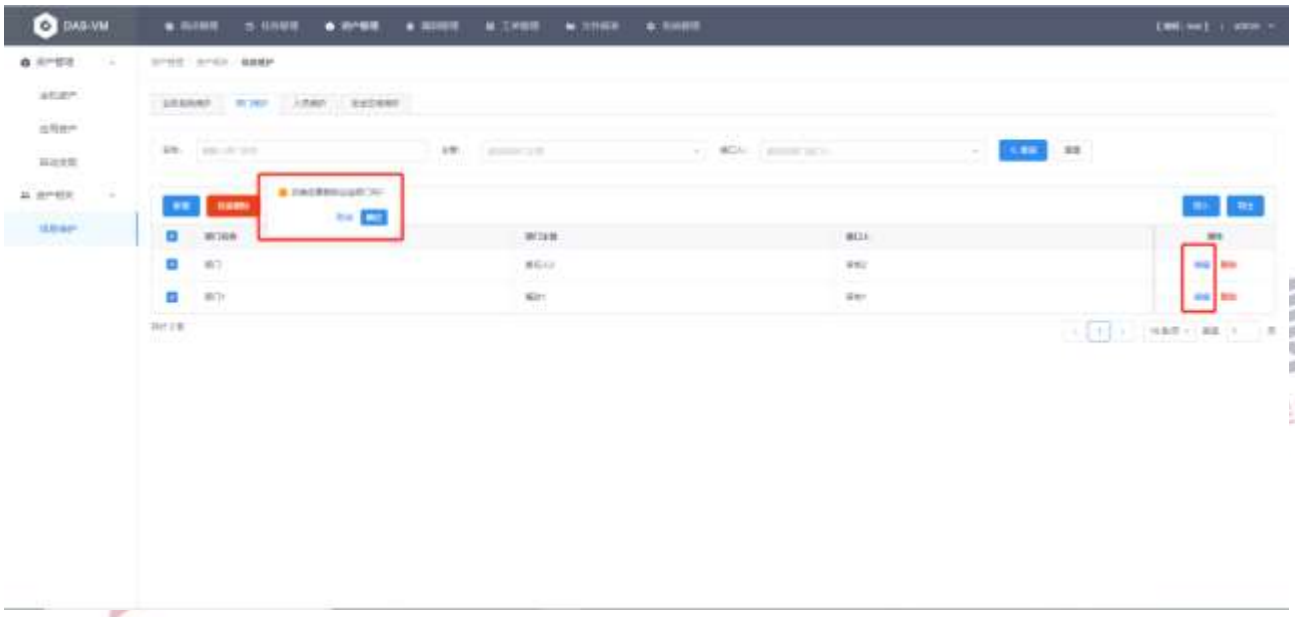
5.2.2.3. 编辑部门

（1） 点击部门列表中的<编辑>按钮，弹出编辑部门窗口，编辑相应的配置项信息，点击<保存>按钮，即可完成部门信息修改。



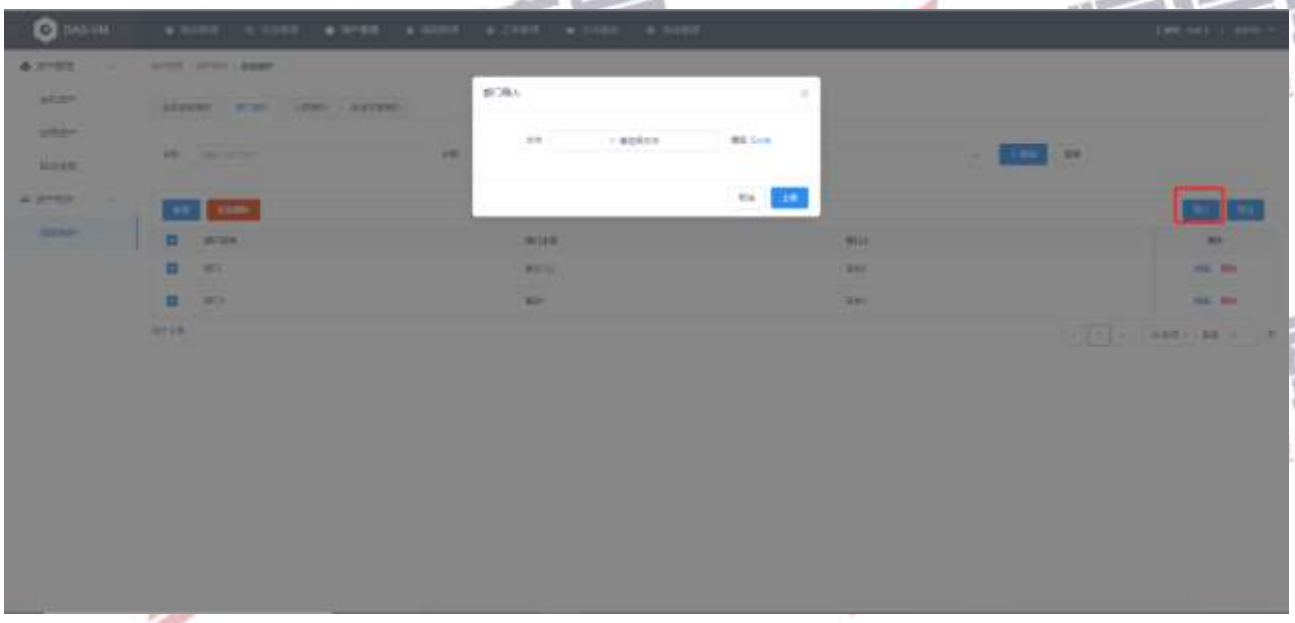
5.2.2.4.5. 删除部门

（1） 点击部门列表中的<删除>按钮并确定，即可删除对应部门。或勾选多个部门后，点击部门列表上面的<批量删除>按钮并确定，即可批量删除选中的部门。



5.2.2.5. 导入导出

（1） 点击<导入>按钮，选择 excel 文件后，点击<上传>按钮可以导入部门，也可以下载模板文件，编辑后再导入。



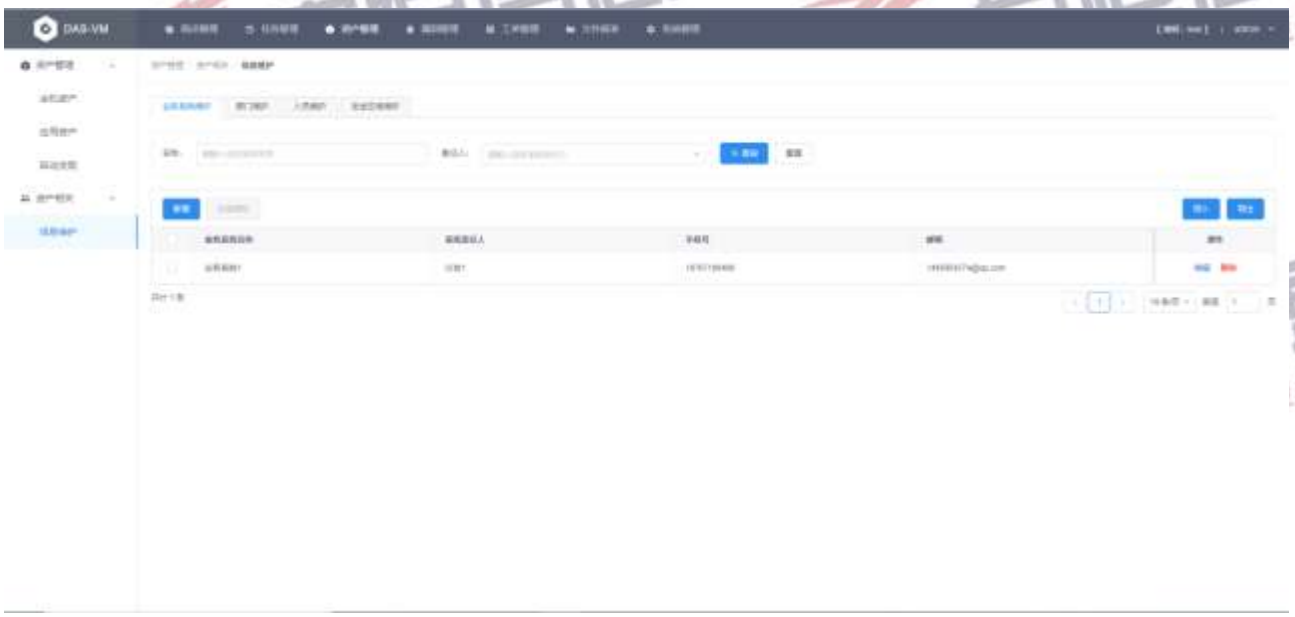
（2） 点击<导出>按钮，可以导出所有部门，页面跳转至[文件报表/报表管理 /下载管理]页面，待进度条达到 100%转绿后，点击<下载>按钮，即可下载导出的部门列表 excel 文件。

5.2.3. 业务系统维护

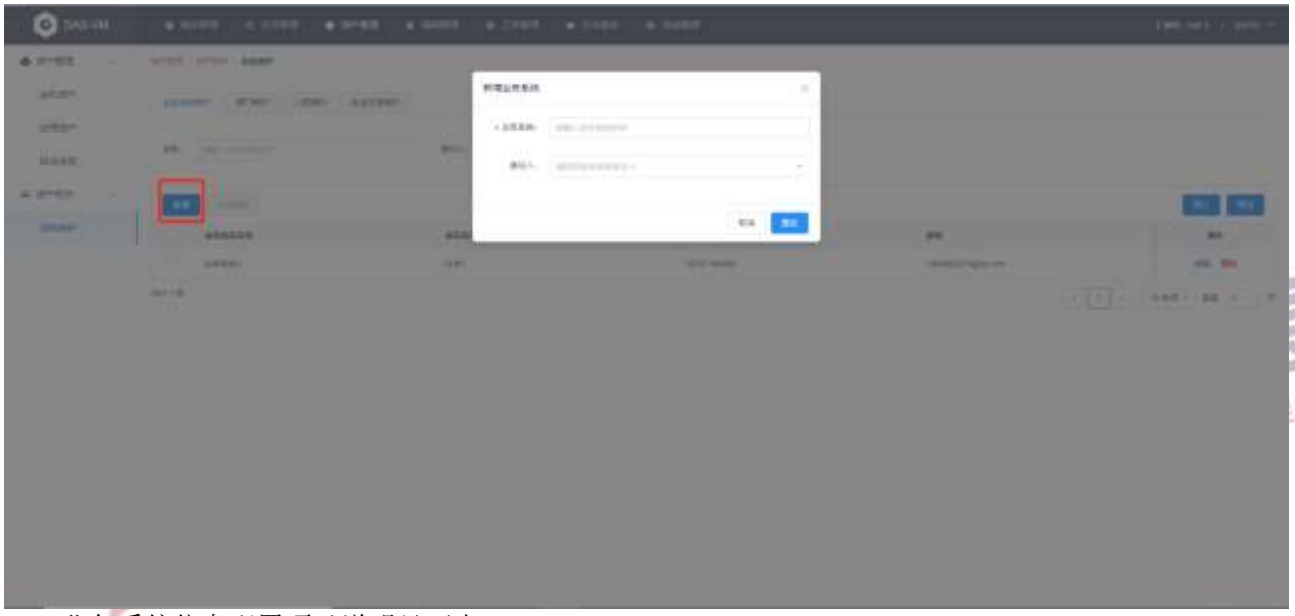
业务系统维护主要用于对业务系统相关信息的增、删、改、查、导入、导出等的管理维护。

5.2.3.1. 新增业务系统

（1） 用户 WEB 登录后，进入[资产管理/资产相关/信息维护]的业务系统维护 tab 页。



（2） 点击<新增>按钮，弹出新增业务系统窗口，填写相应的信息，点击<保存>按钮，即可完成业务系统添加。

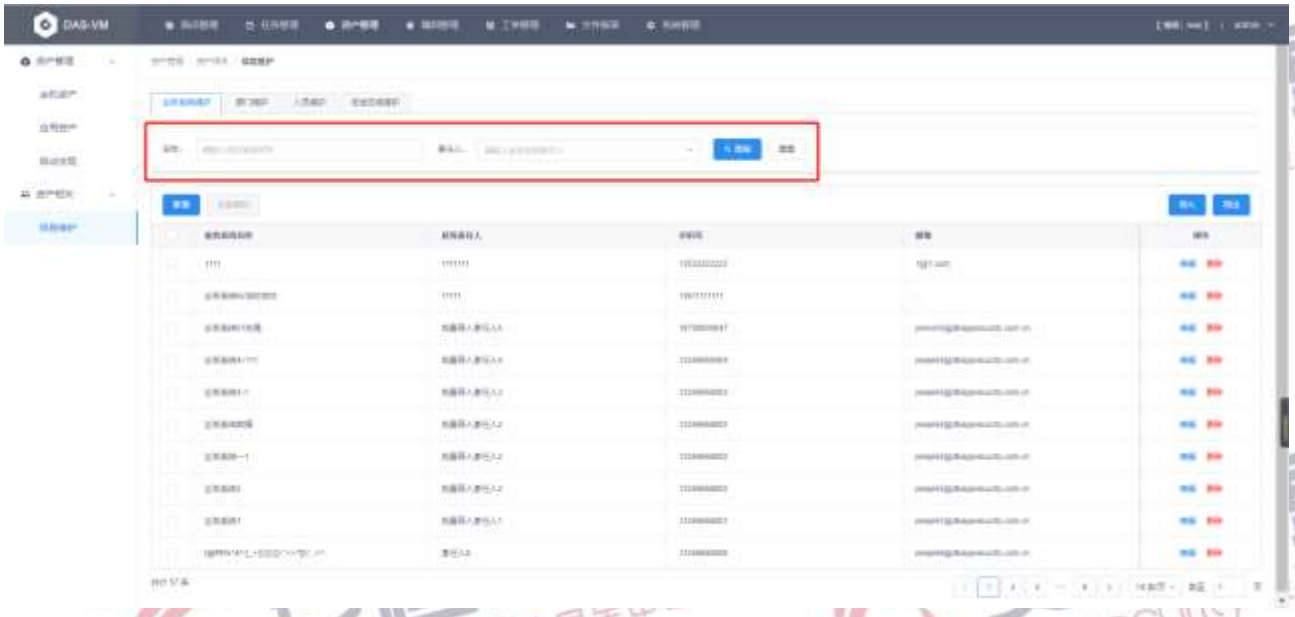


业务系统信息配置项及说明见下表：

配置项	说明
业务系统	必填项。填写业务系统名称
责任人	选填项。选择业务系统的责任人

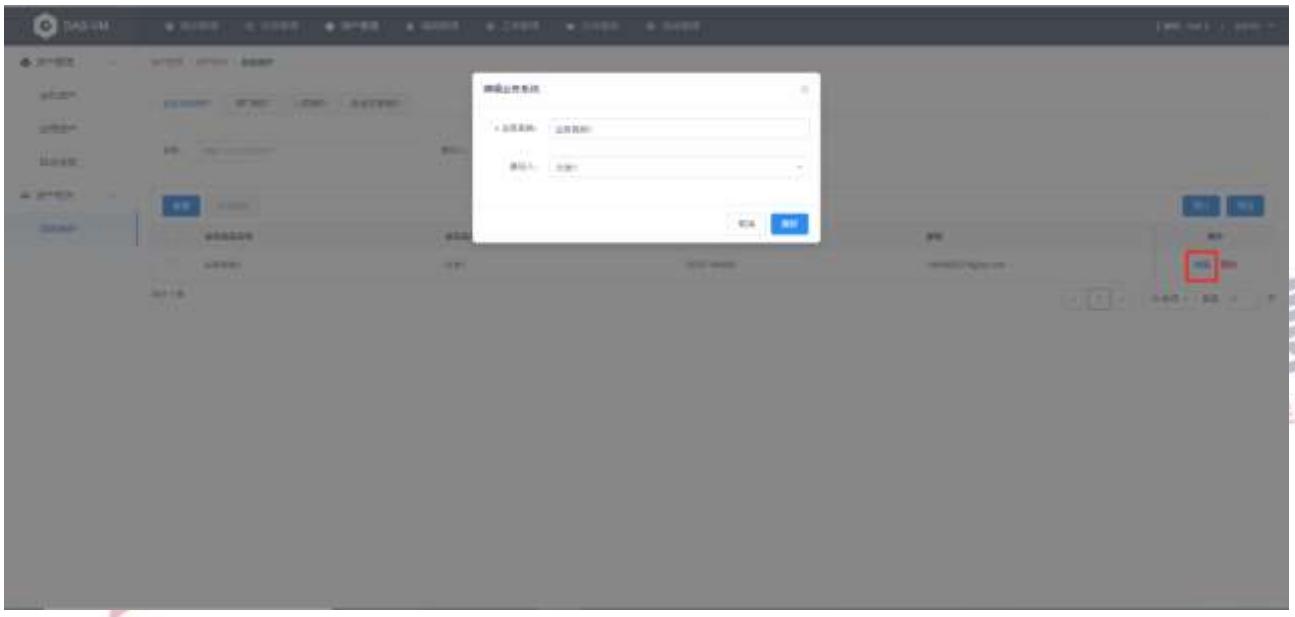
5.2.3.2. 查询业务系统

（1）设置查询条件，可在业务系统维护列表中进行指定业务系统查询，条件设置后，点击<查询>按钮，进行查询。点击<重置>按钮，可清空查询条件。



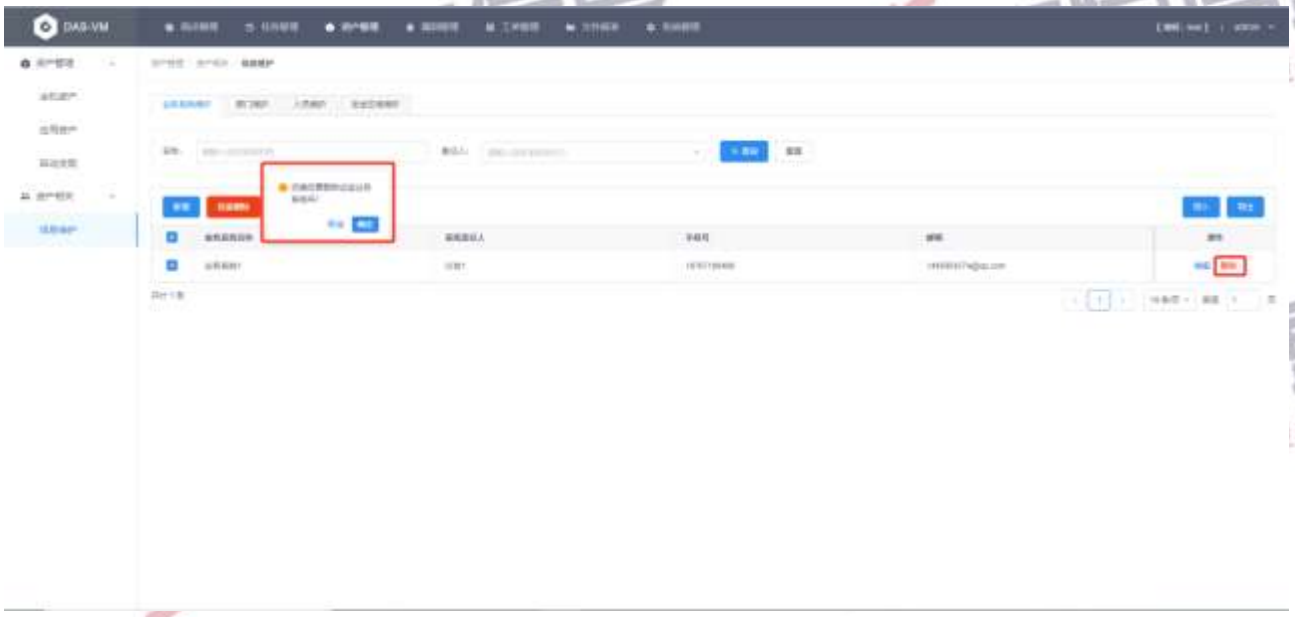
5.2.3.3. 编辑业务系统

（1） 点击业务系统列表中的<编辑>按钮，弹出编辑业务系统窗口，编辑相应的配置项信息，点击<保存>按钮，即可完成业务系统信息修改。



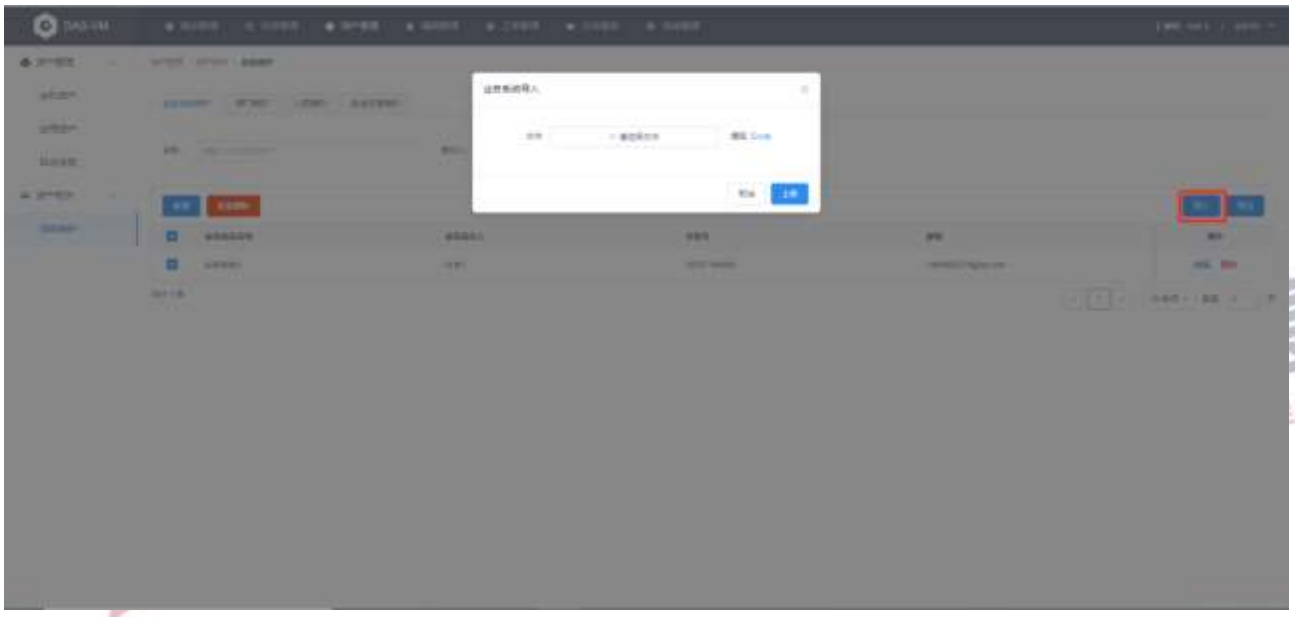
5.2.3.4. 删除业务系统

（1） 点击业务系统列表中的<删除>按钮并确定，即可删除对应业务系统。或勾选多个业务系统点击业务系统列表上面的<批量删除>按钮并确定，即可批量删除选中的业务系统。

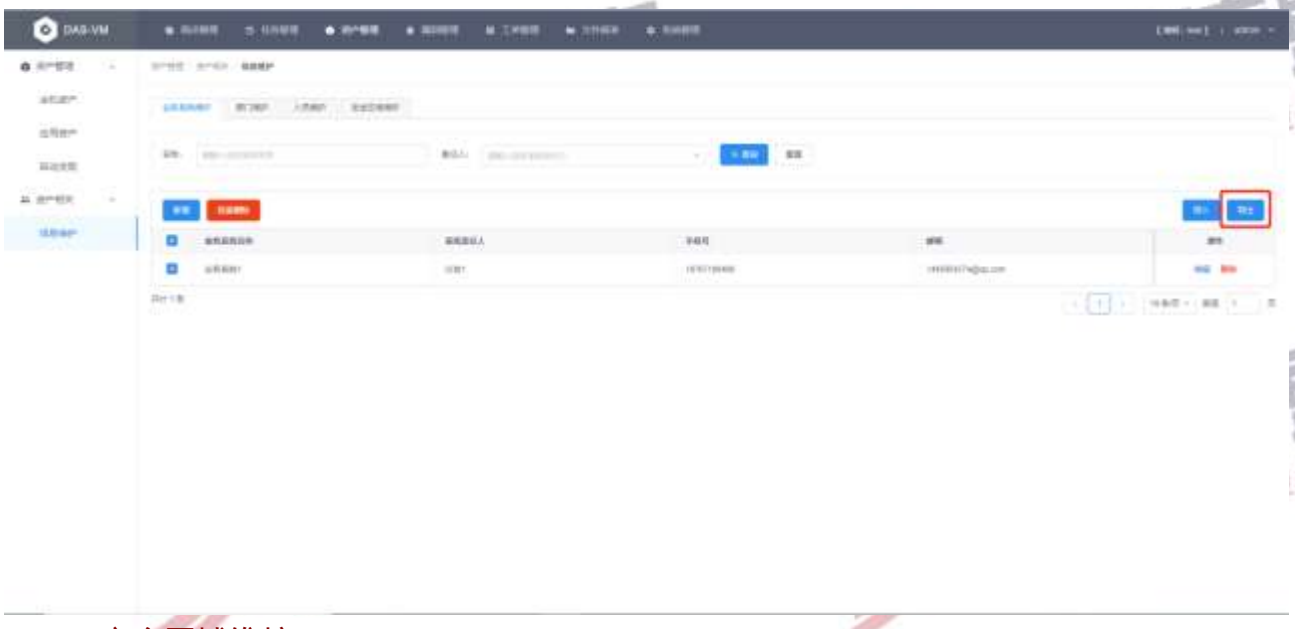


5.2.3.5. 导入导出

（1） 点击<导入>按钮，选择 excel 文件后，点击<上传>按钮可以导入业务系统，也可以下载模板文件，编辑后再导入。



（2） 点击<导出>按钮，可以导出所有业务系统，页面跳转至[文件报表/报表管理 /下载管理]页面，待进度条达到 100%转绿后，点击<下载>按钮，即可下载导出的业务系统列表 excel 文件。

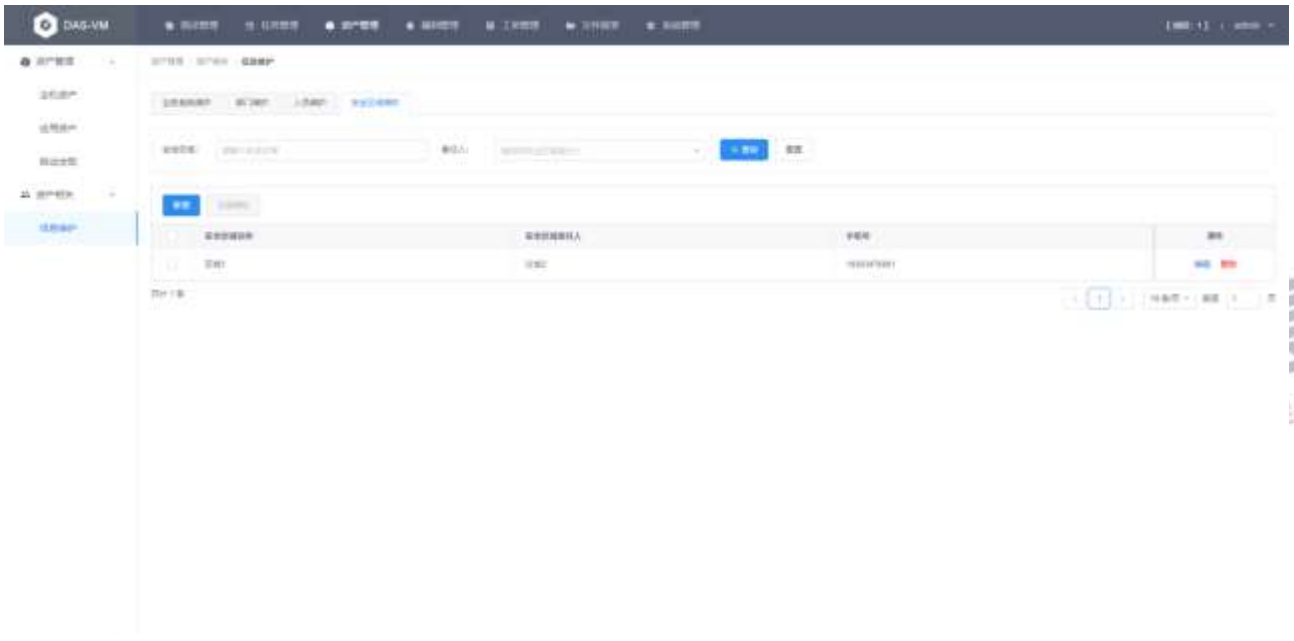


5. 2. 4. 安全区域维护

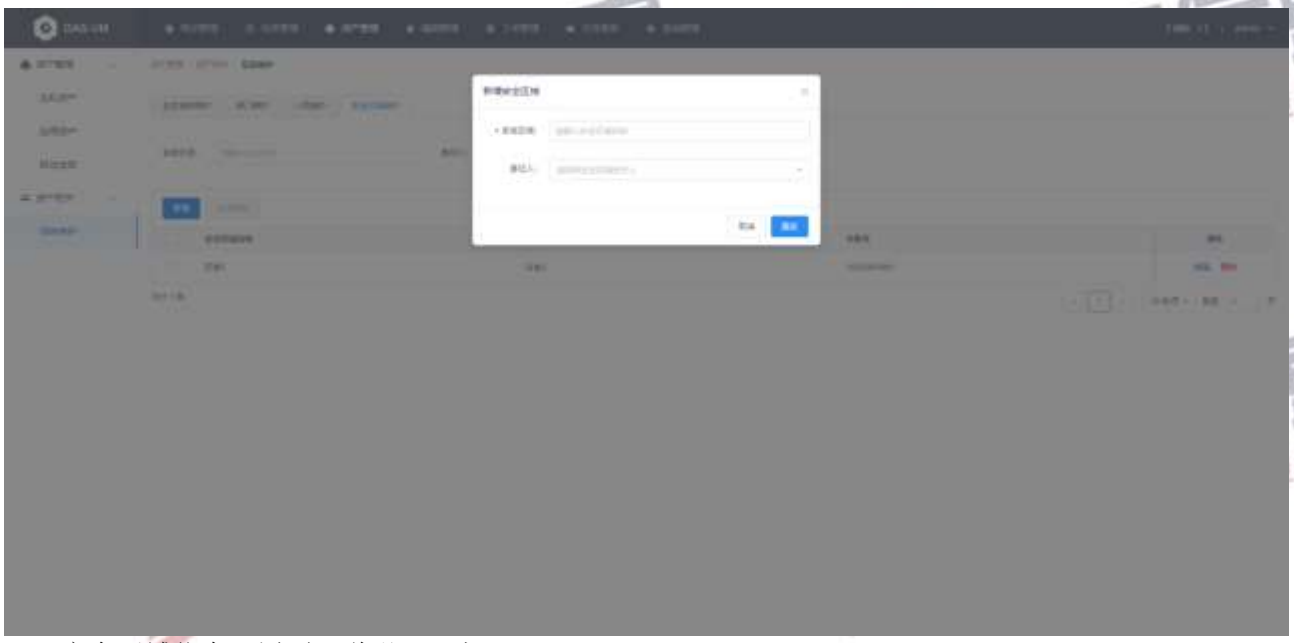
安全区域维护主要用于对安全区域相关信息的增、删、改、查等的管理维护。

5.2.4.1. 新增安全区域

（1） 用户 WEB 登录后，进入[资产管理/资产相关/信息维护]的安全区域维护 tab 页。



（2）点击<新增>按钮，弹出新增安全区域窗口，填写相应的信息，点击<保存>按钮，即可完成安全区域添加。

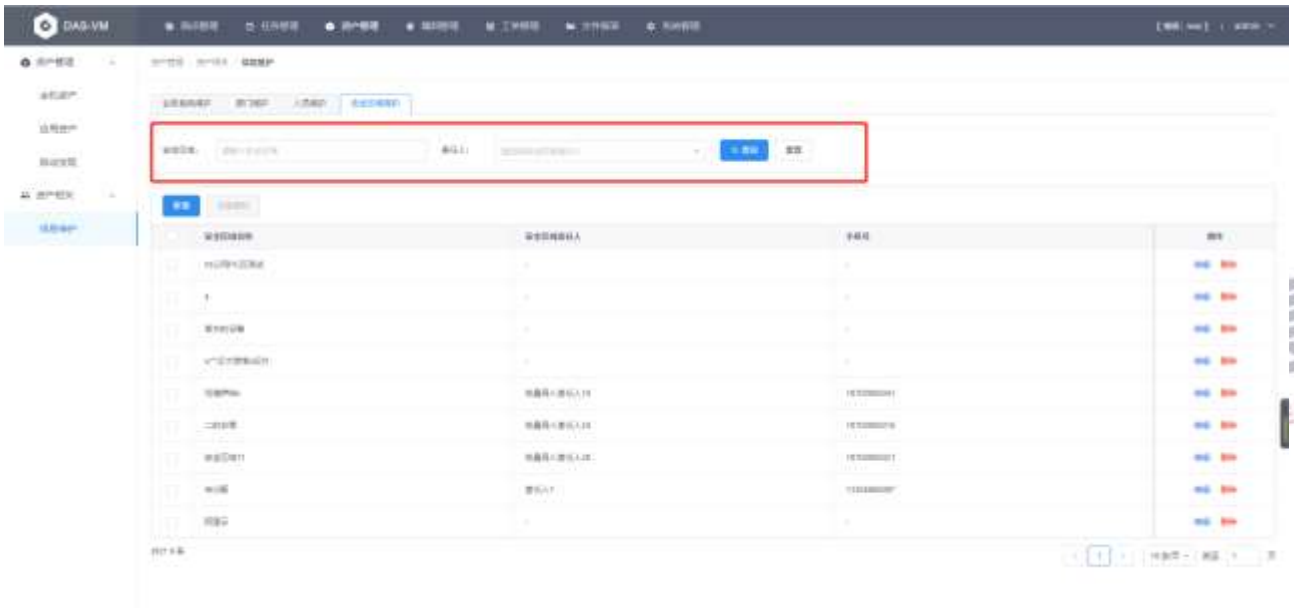


安全区域信息配置项及说明见下表：

配置项	说明
安全区域	必填项。填写安全区域名称。
责任人	选填项。选择安全区域的责任人。

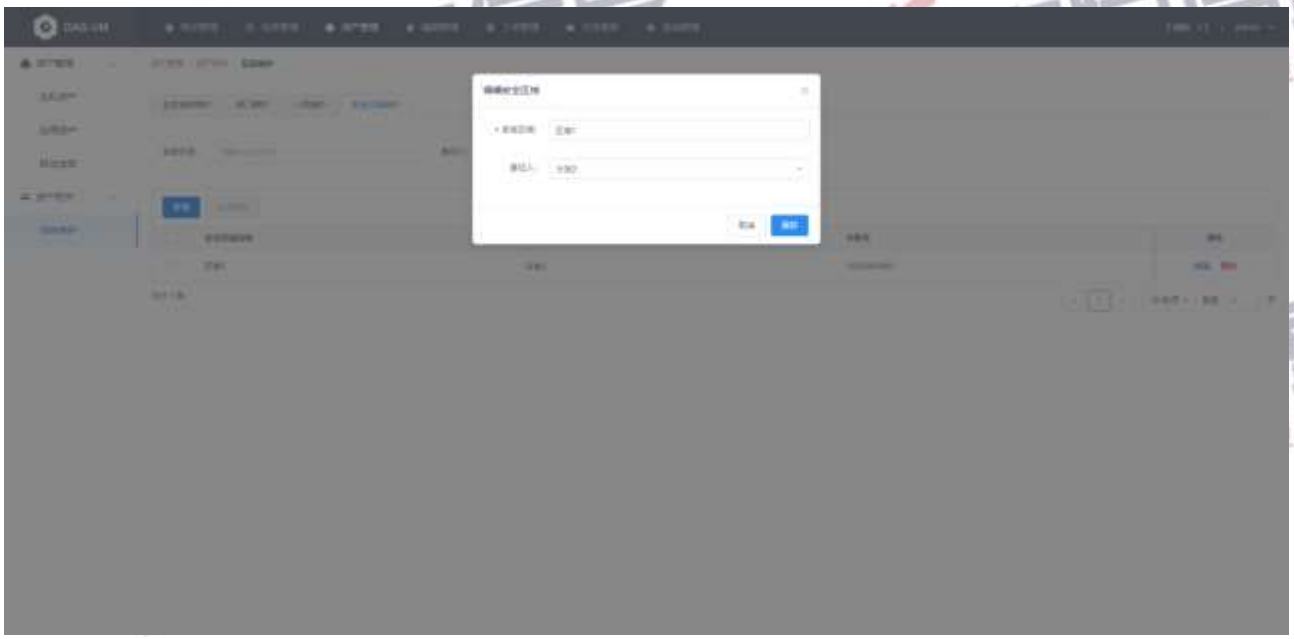
5.2.4.2. 查询安全区域

（1）设置查询条件，可在安全区域维护列表中进行指定安全区域查询，条件设置后，点击<查询>按钮，进行查询。点击<重置>按钮，可清空查询条件。



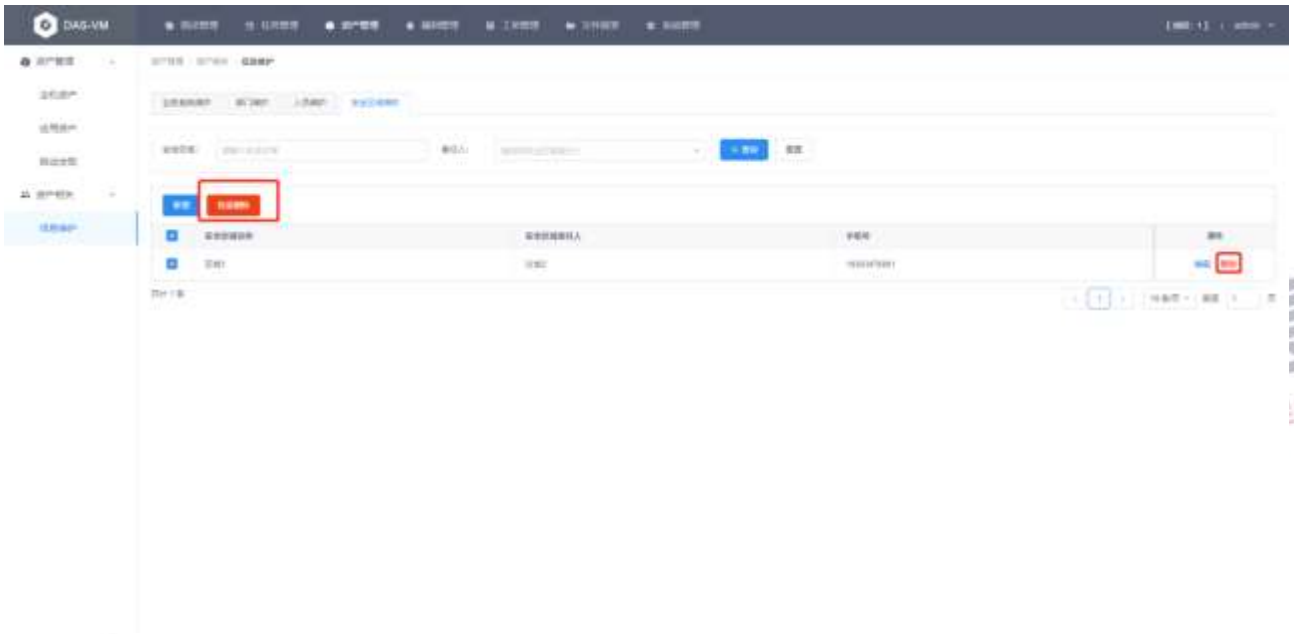
5.2.4.3. 编辑安全区域

（1）点击安全区域列表中的<编辑>按钮，弹出编辑安全区域窗口，编辑相应的配置项信息，点击<保存>按钮，即可完成安全区域信息修改。



5.2.4.4. 删除安全区域

（1）点击安全区域列表中的<删除>按钮并确定，即可删除对应安全区域。或勾选多个安全区域点击安全区域列表上面的<批量删除>按钮并确定，即可批量删除选中的安全区域。



6. 漏洞管理

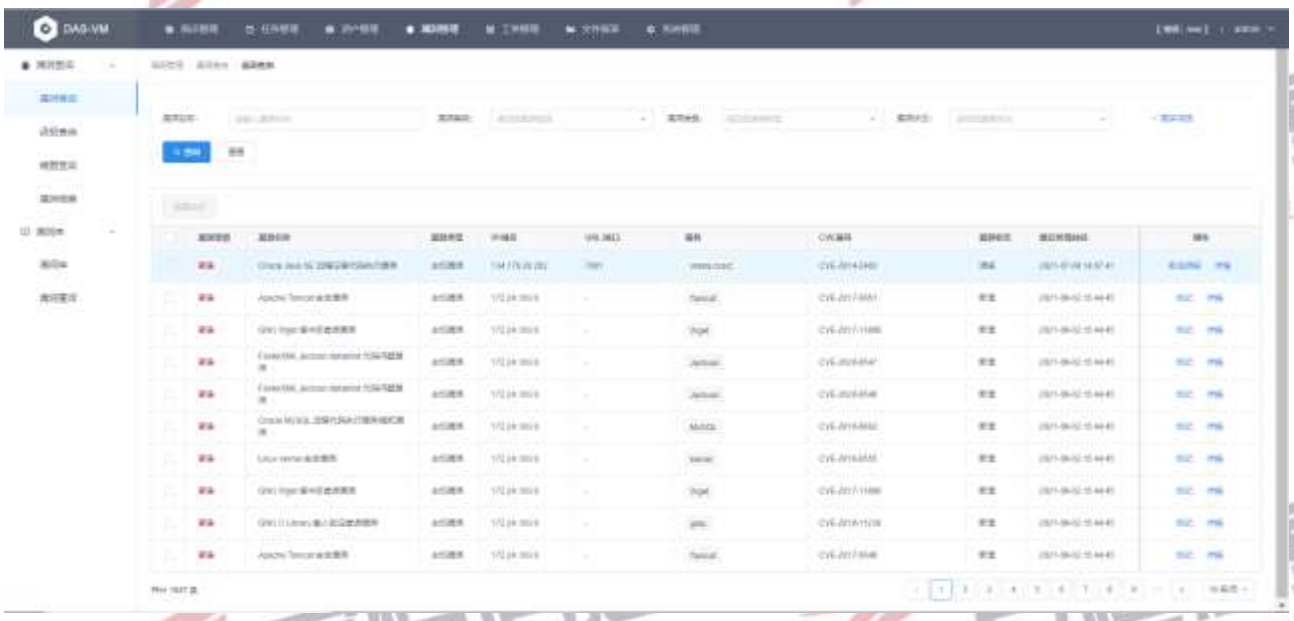
6.1. 漏洞查询

漏洞库中记录了所有扫描引擎扫描出来的漏洞信息

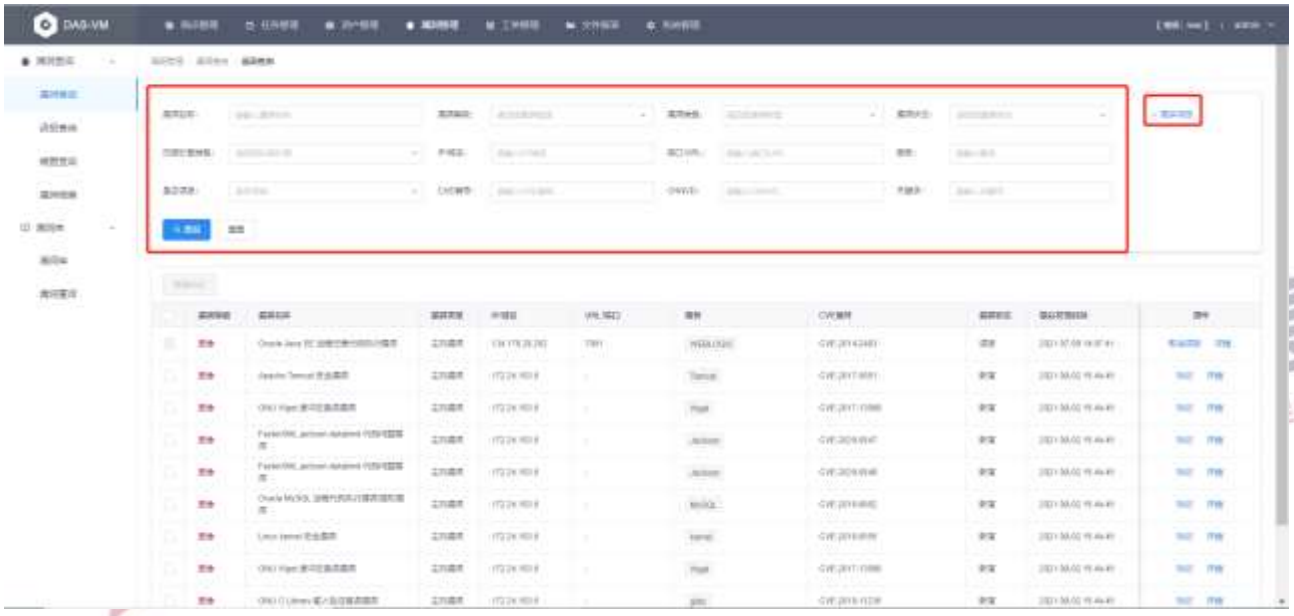
6. 1. 1. 漏洞查询

6.1.1.1. 漏洞查询

（1） 用户 WEB 登录后，进入[漏洞管理 /漏洞查询 /漏洞查询]页面。

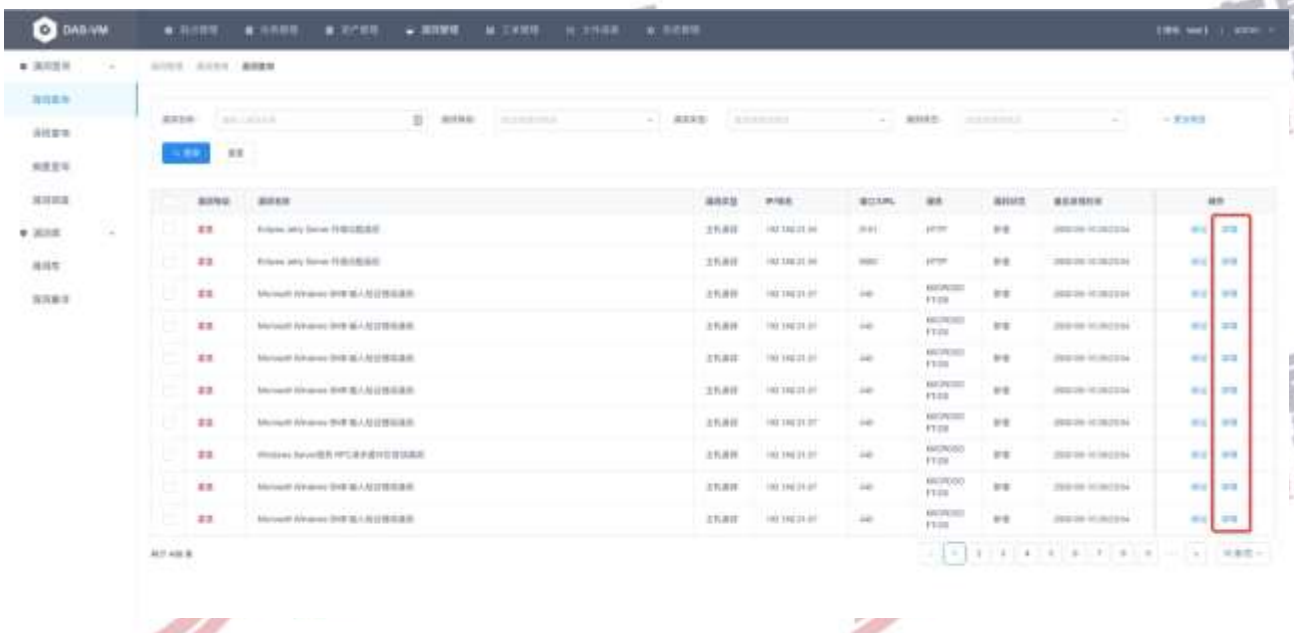


（2）设置查询条件，可在漏洞库中进行指定漏洞查询，条件设置后，点击<查询>按钮，进行查询。也可点击<更多筛选>按钮，下拉展开更多的查询条件，设置条件后，点击<查询>按钮，进行查询。

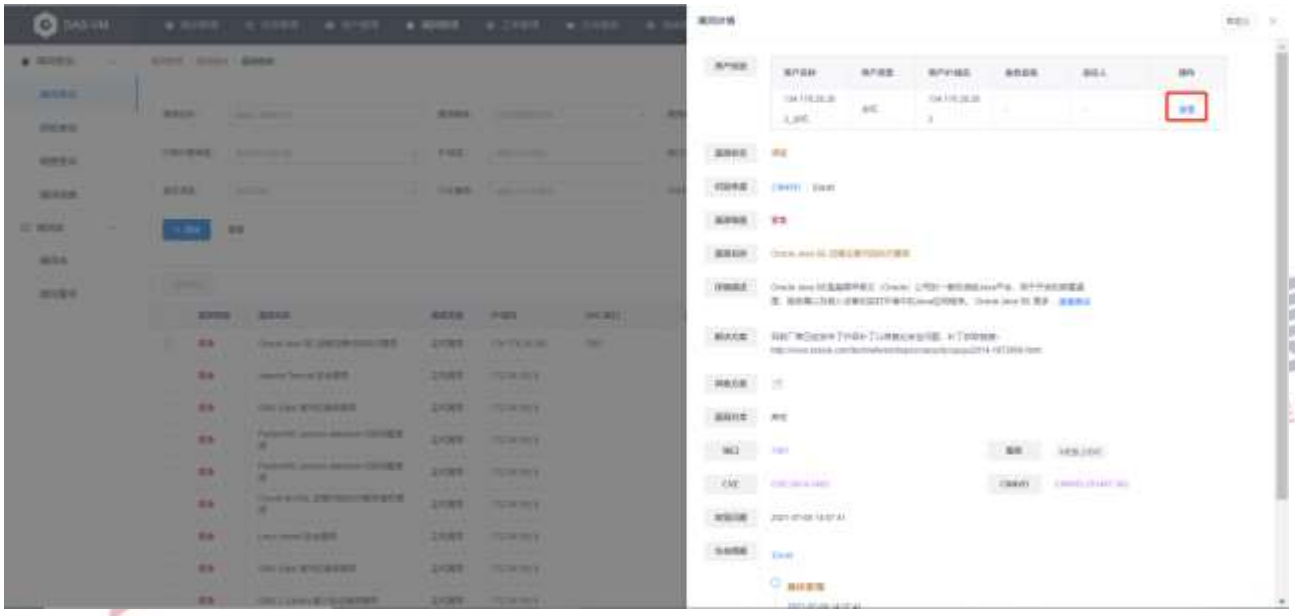


6.1.1.2. 漏洞详情

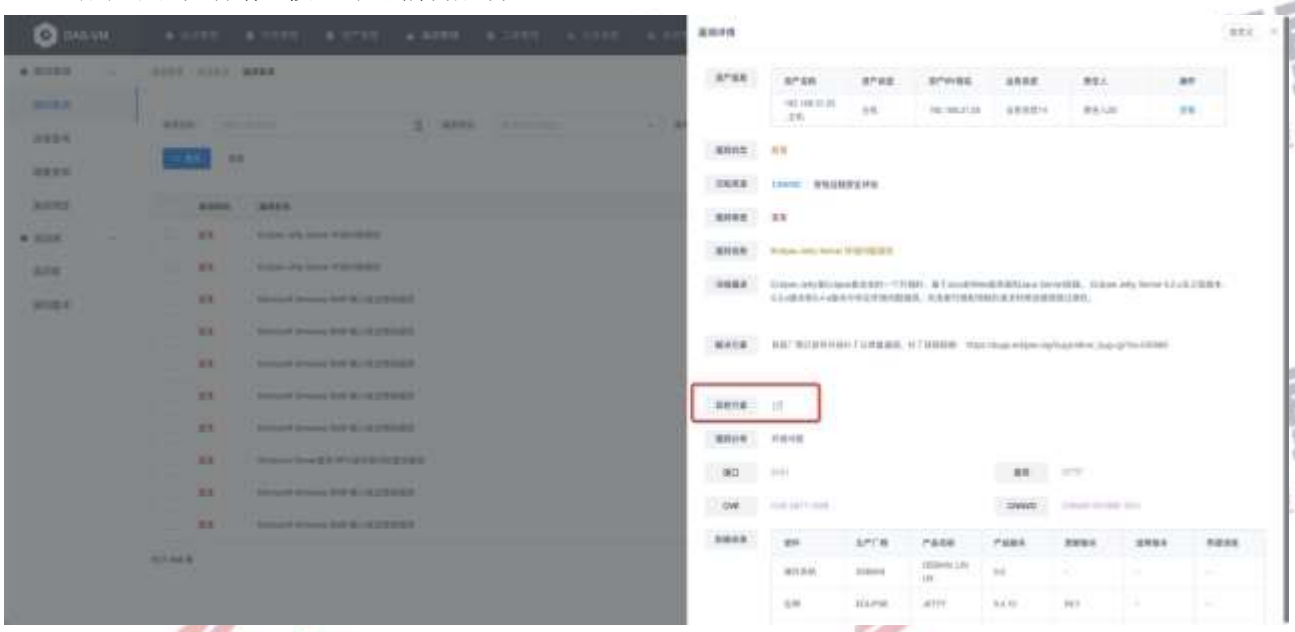
（1） 点击漏洞列表中的<详情>按钮，可以查看对应漏洞的详细信息。



（2） 点击资产相关信息列表中的<查看>按钮，可以查看漏洞所属资产的相关详细信息。

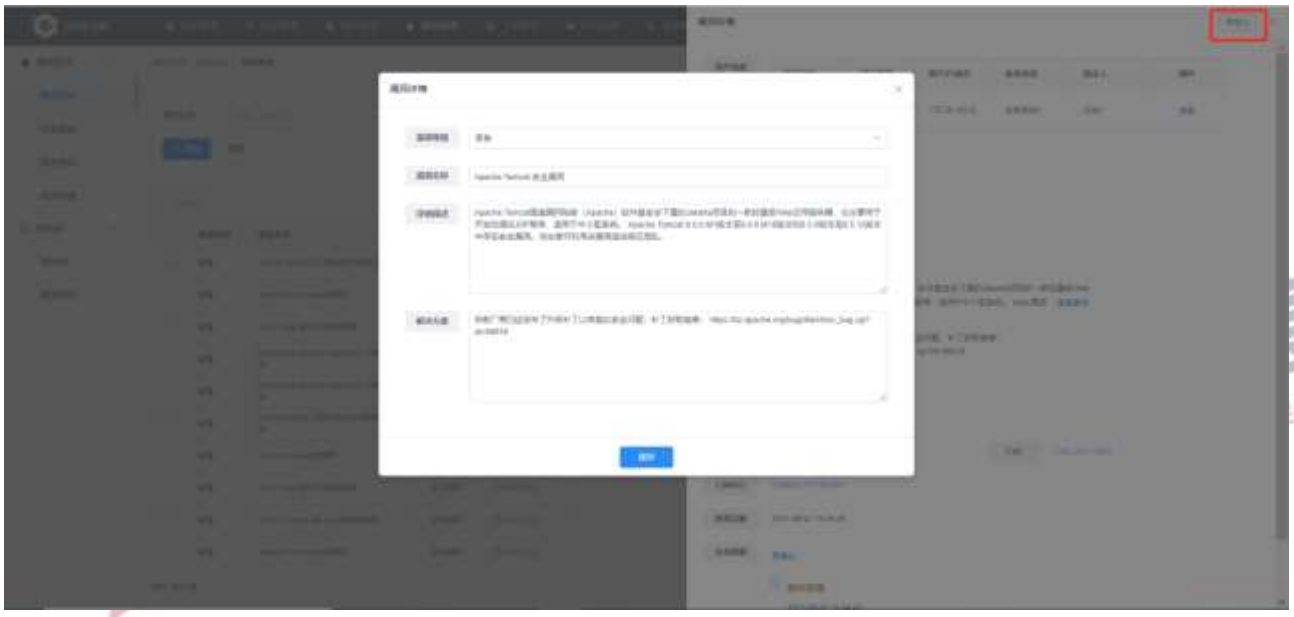


（3） 点击其他方案栏编辑图标可添加或编辑其他解决方案。其他方案栏支持图片和文本形式，编辑完成后点击<保存>按钮即可编辑成功。



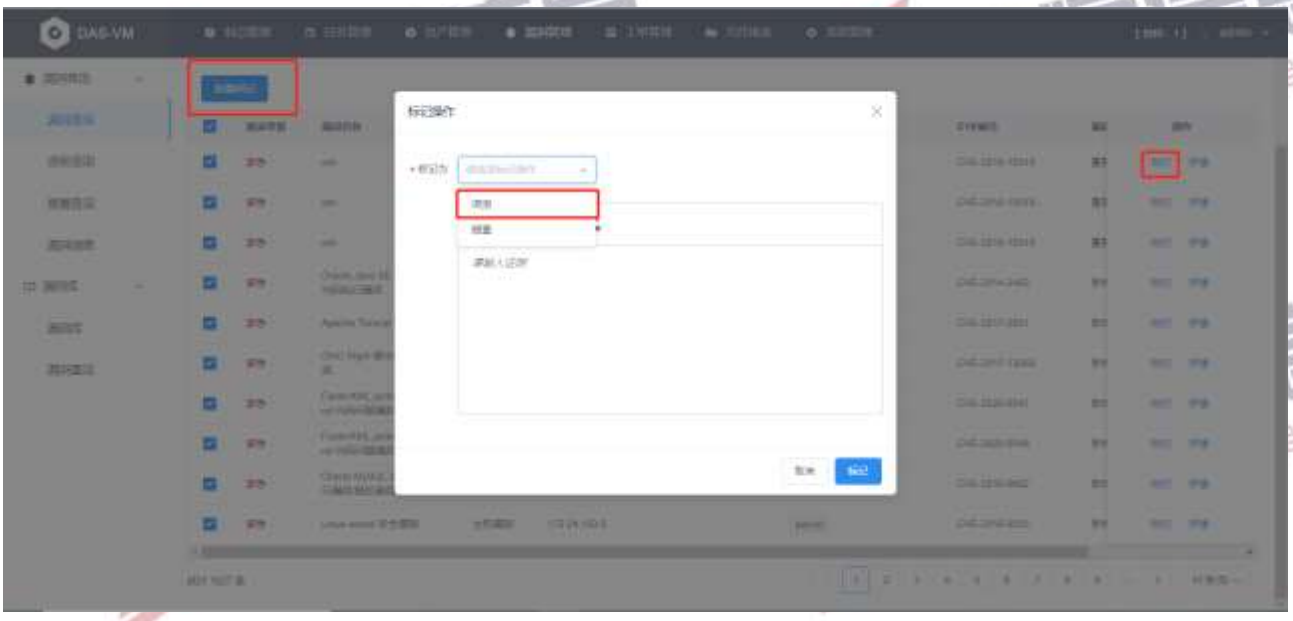
6.1.1.3. 漏洞自定义

（1） 点击漏洞详情中的<自定义>按钮，可自定义漏洞等级、漏洞名称、详细描述和解决方案。

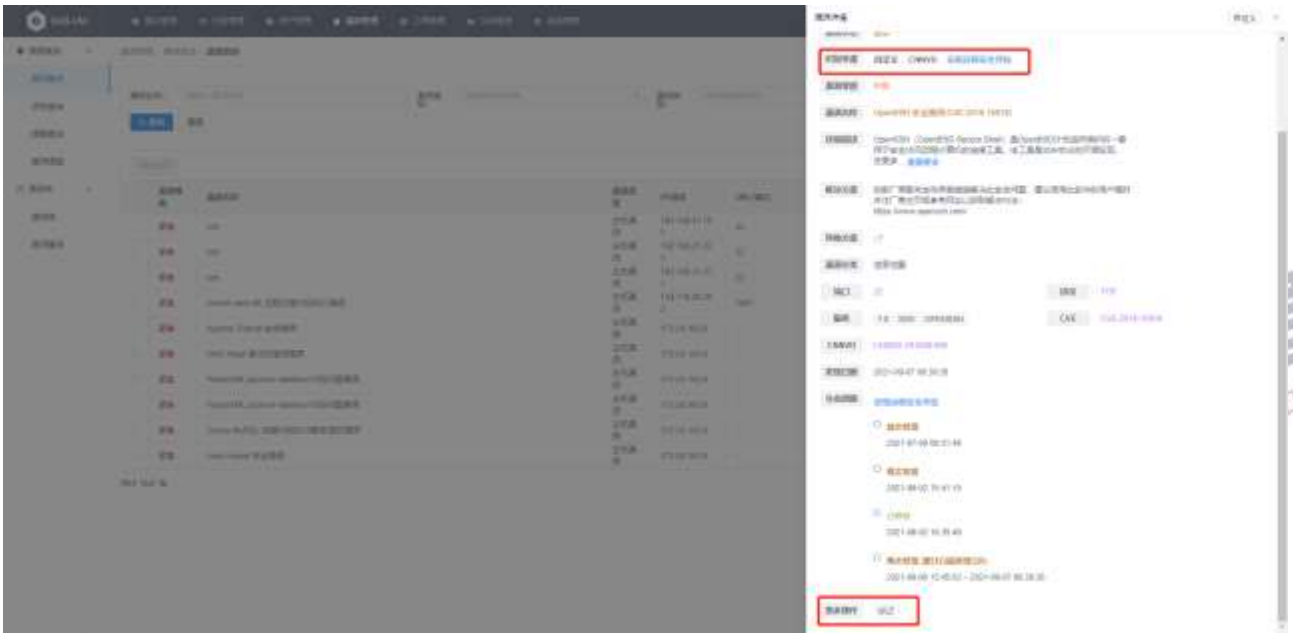


6.1.1.4. 标记误报

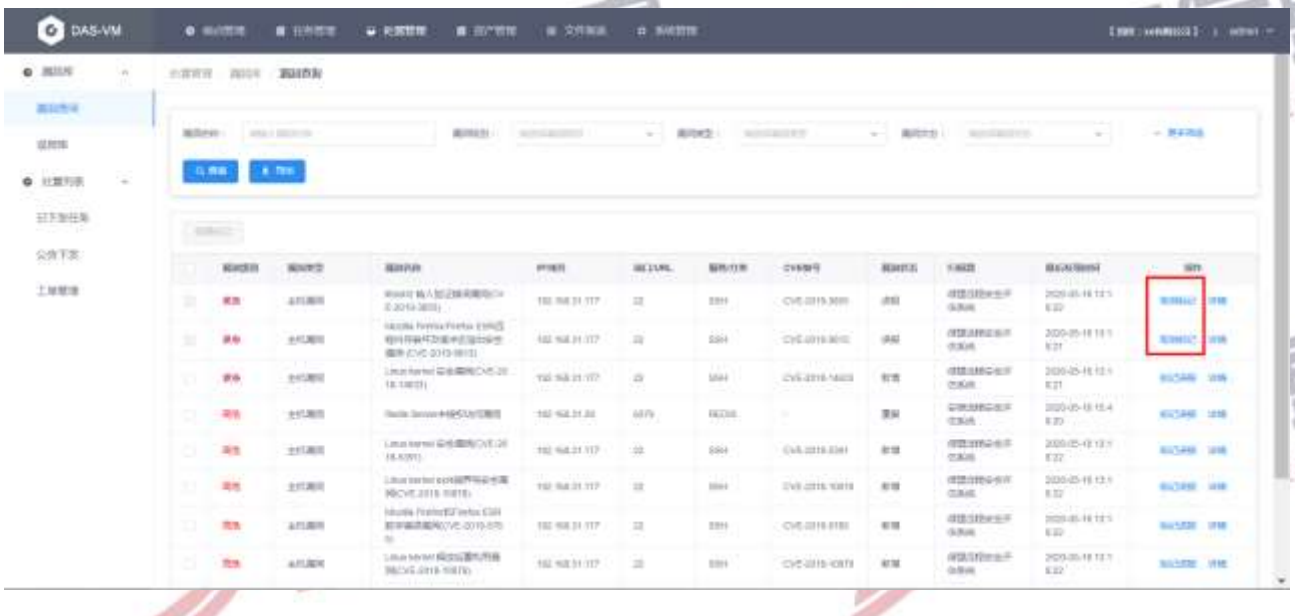
（1） 点击漏洞列表中的<标记>按钮或勾选漏洞点击<批量标记>按钮，并输入描述信息，可以将选择的漏洞单个或批量标记成为误报漏洞，此时标记的误报是将不同扫描引擎下的漏洞均标记为误报。



（2） 点击漏洞列表中的<详情>，选择[识别来源]的自定义和 CNNVD 进行[更多操作]时，是将所有扫描引擎下的漏洞全部标记为误报，但是选择[识别来源]的不同扫描引擎，如安恒远程安全评估，进行[更多操作]标记为误报仅仅是对该扫描引擎下的漏洞进行了误报标记。

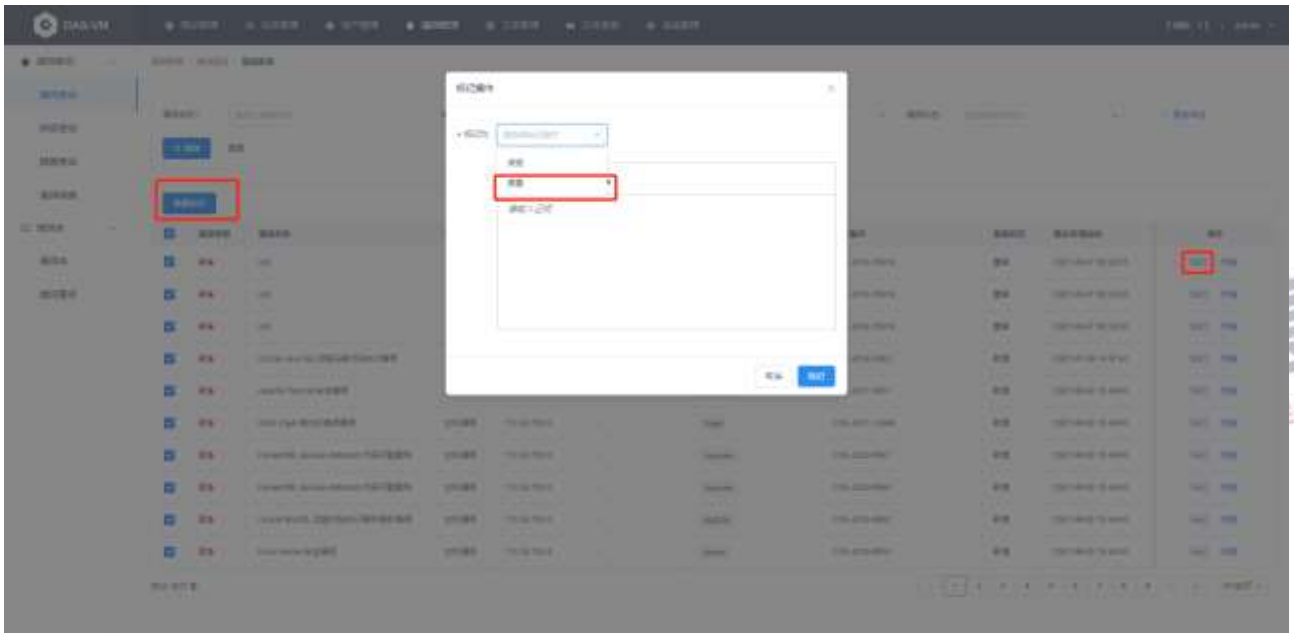


（3） 误报漏洞操作列<标记误报>按钮变更为<取消误报>按钮，点击<取消误报>按钮，可以取消误报标记（搁置漏洞不会展示取消标记按钮）。



6.1.1.5. 标记搁置

（1） 点击漏洞列表中的<标记>按钮或勾选漏洞点击<批量标记>按钮，并输入描述信息，可以将选择的漏洞单个或批量标记成为搁置漏洞，或者点击漏洞列表中的<详情>，进入漏洞详情页，在更多操作中进行标记，这两种标记方式把不同扫描引擎下的漏洞均标记为搁置。

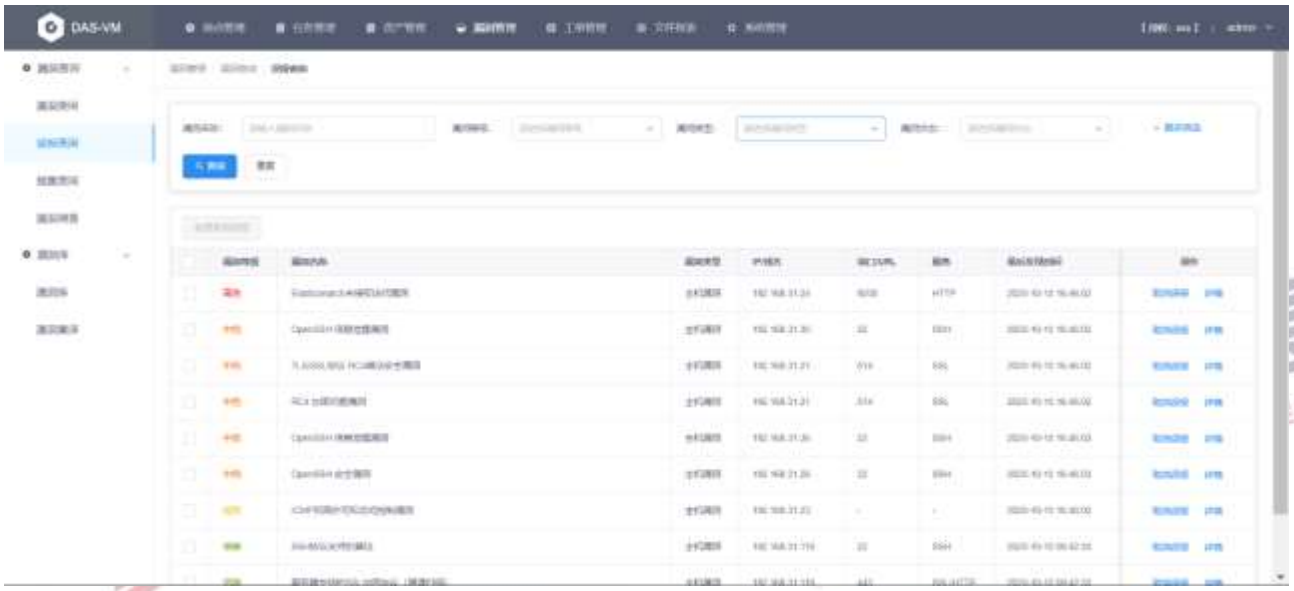


（2）搁置漏洞不会在漏洞列表页展示取消标记按钮，但是在漏洞详情页出现<取消搁置>按钮，点击<取消搁置>按钮可以取消对漏洞的搁置标记。

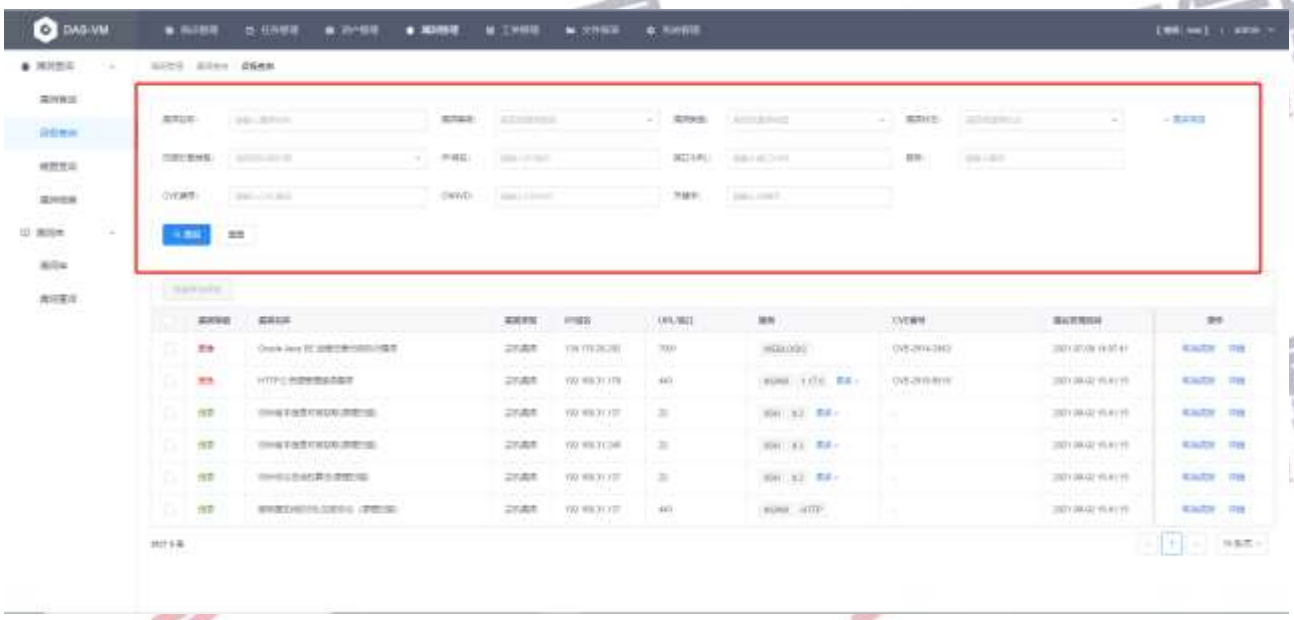
6. 1. 2. 误报查询

6.1.2.1. 误报漏洞查询

（1） 用户 WEB 登录后，进入[漏洞管理 /漏洞查询 /误报查询]页面。

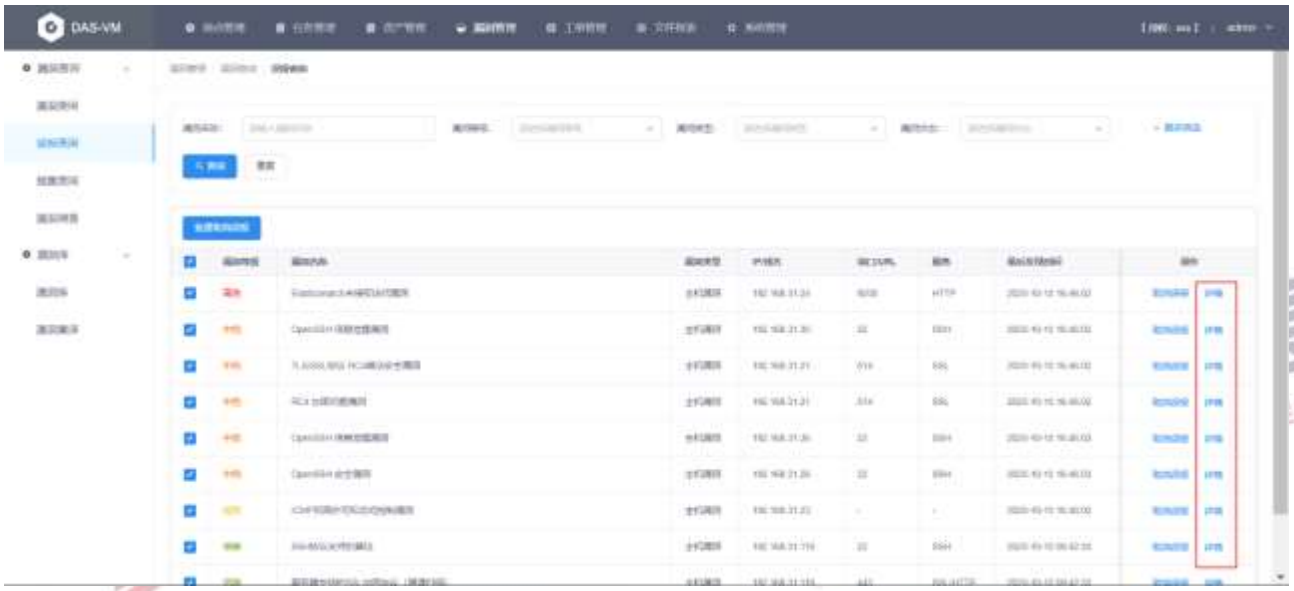


（2）设置查询条件，可在误报库中进行指定误报漏洞查询，条件设置后，点击<查询>按钮，进行查询。也可点击<更多筛选>按钮下拉展开更多的查询条件，设置条件后，点击<查询>按钮，进行查询。

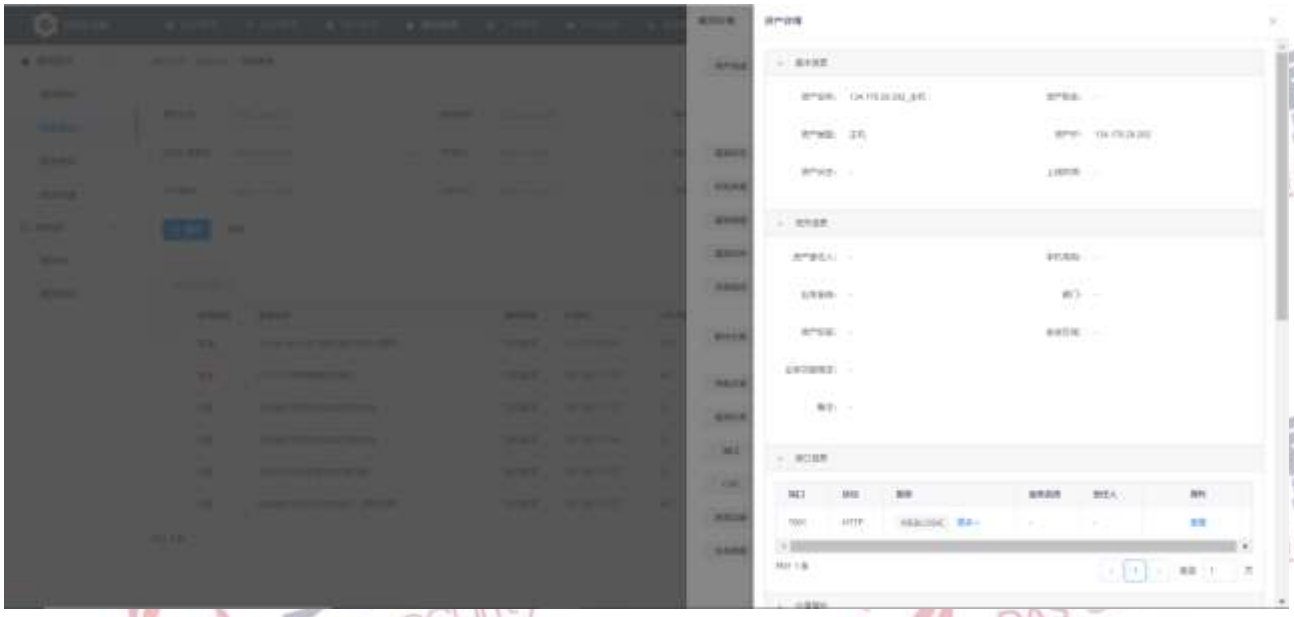


6.1.2.2. 误报漏洞详情

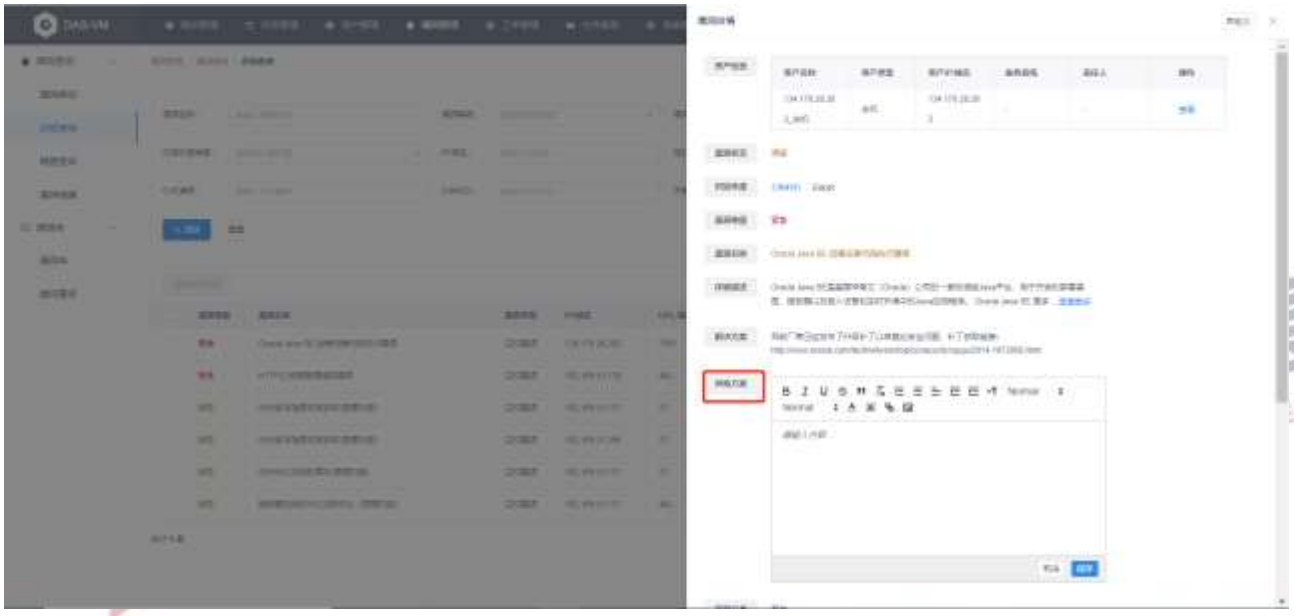
（1） 点击误报漏洞列表中操作列的<查看>按钮，可以查看对应误报漏洞的详细信息。



（2） 点击资产相关信息列表中的<查看>按钮，可以查看误报漏洞所属资产的相关详细信息。

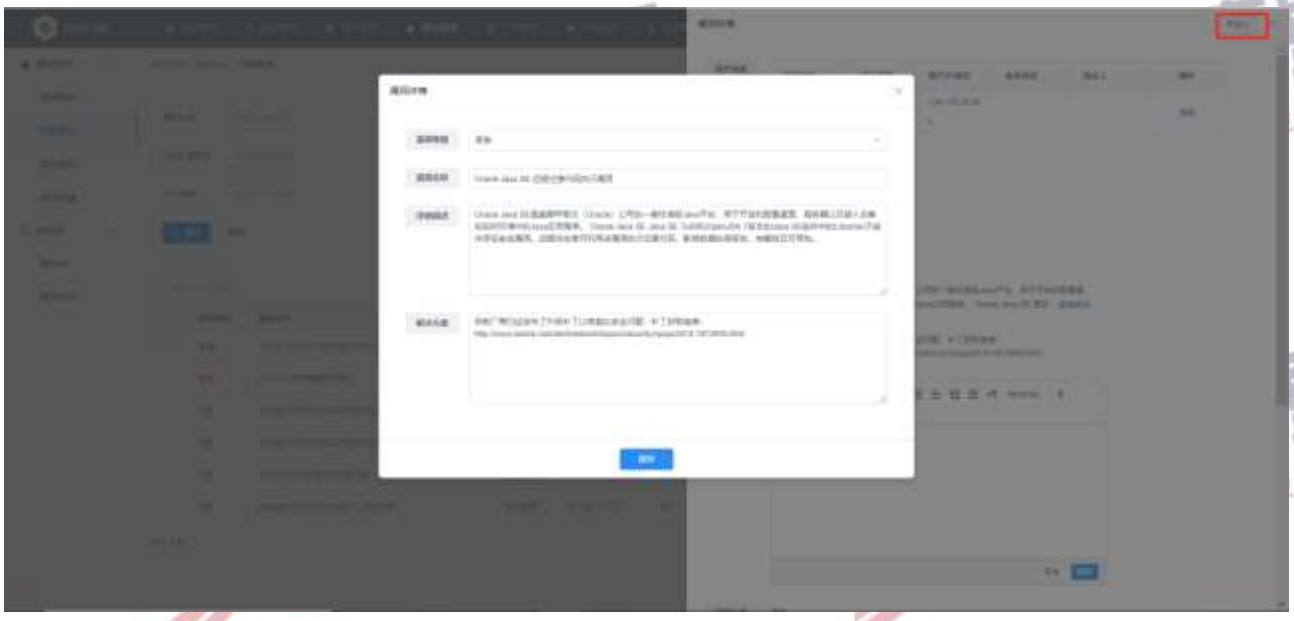


（3） 点击其他方案栏编辑图标可添加或编辑其他解决方案。其他方案栏支持图片和文本形式，编辑完成后点击<保存>按钮即可编辑成功。



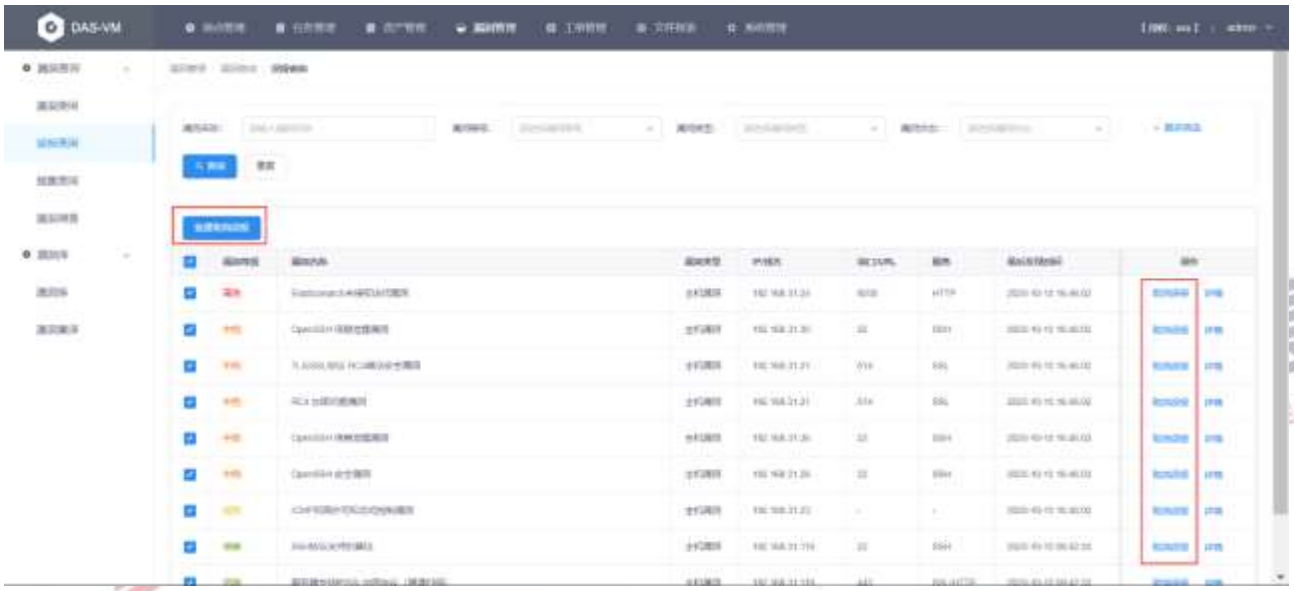
6.1.2.3. 漏洞自定义

（1） 点击漏洞详情中的<自定义>按钮，可自定义漏洞等级、漏洞名称、详细描述和解决方案。



6.1.2.4. 取消误报

（1） 点击误报漏洞列表中的<取消标记>按钮或勾选误报漏洞点击<批量取消标记>按钮，可以将选择的漏洞单个或批量取消误报标记，并从误报库剔除。

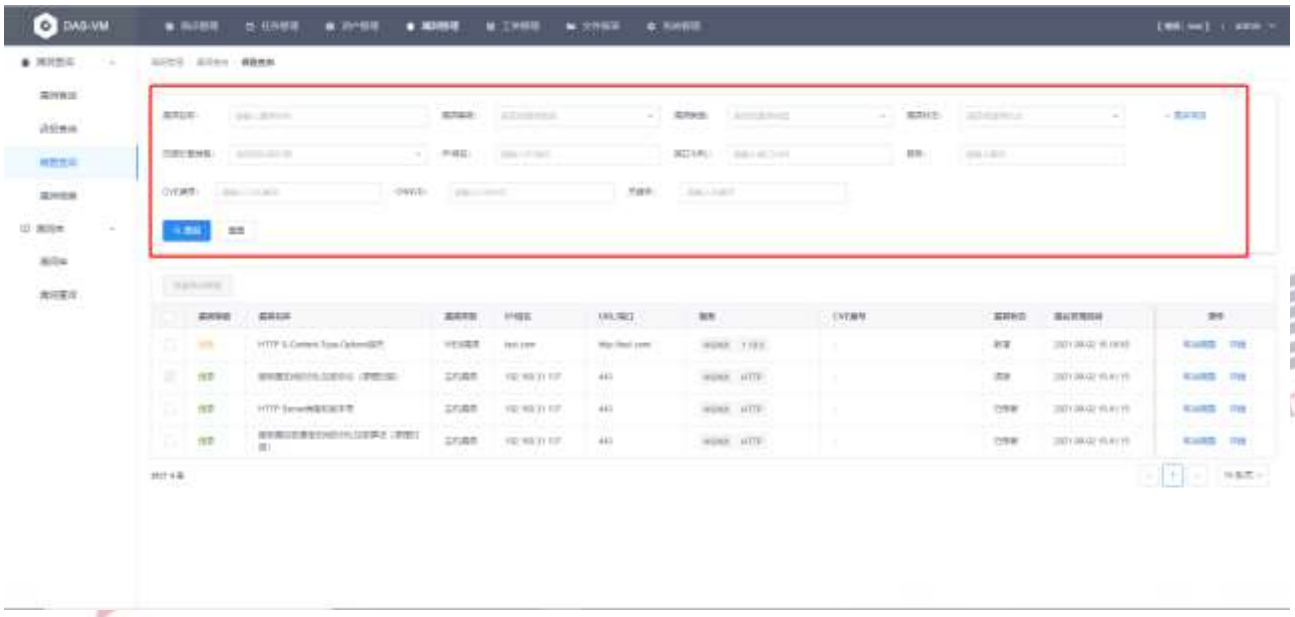


6. 1. 3. 搁置查询

6.1.3.1. 搁置漏洞查询

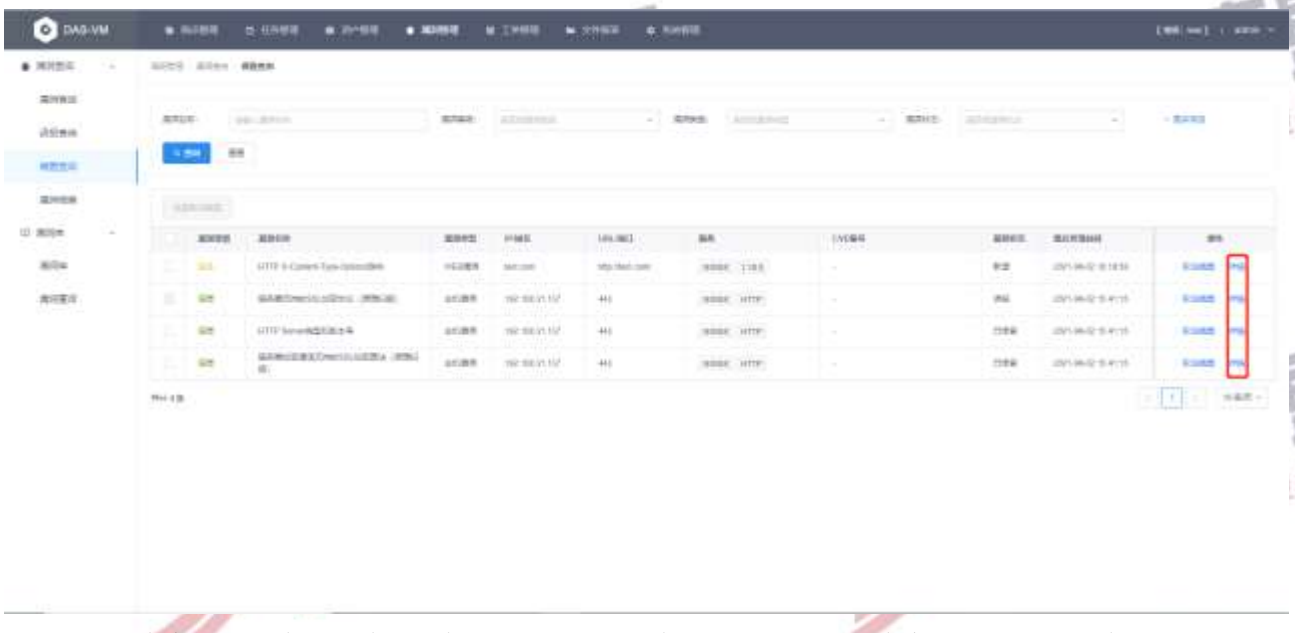
（1） 用户 WEB 登录后，进入[漏洞管理 /漏洞查询 /搁置查询]页面。

（2） 设置查询条件，可在搁置库中进行指定搁置漏洞查询，条件设置后，点击<查询>按钮，进行查询。也可点击<更多筛选>按钮下拉展开更多的查询条件，设置条件后，点击<查询>按钮，进行查询。

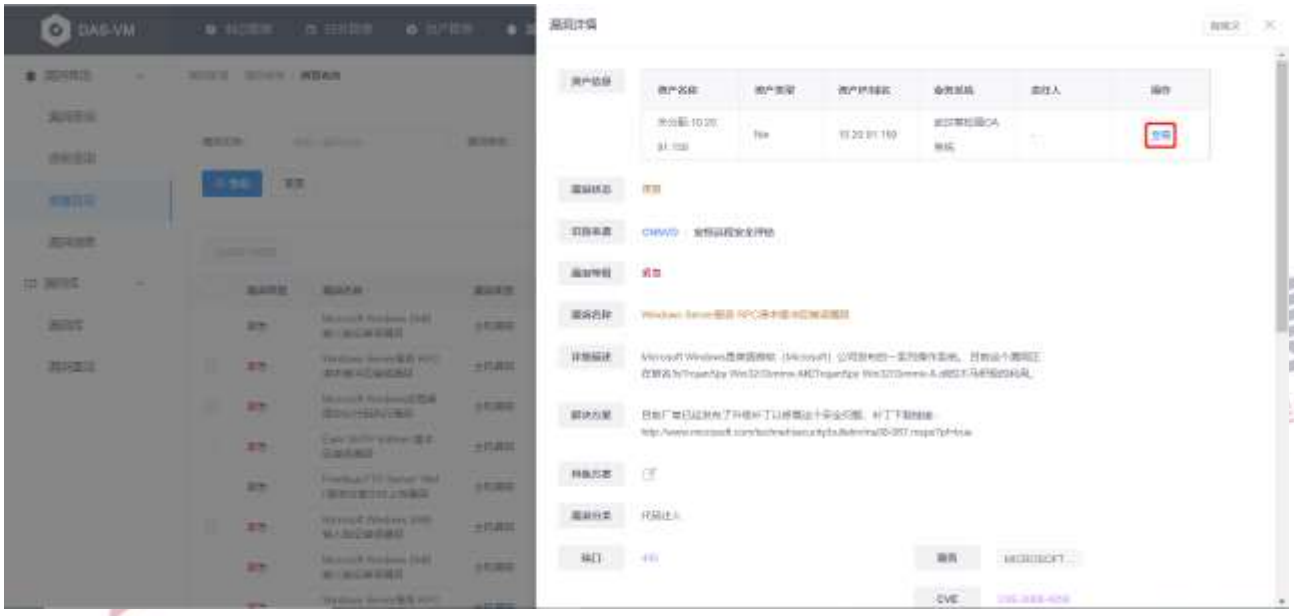


6.1.3.2. 搁置漏洞详情

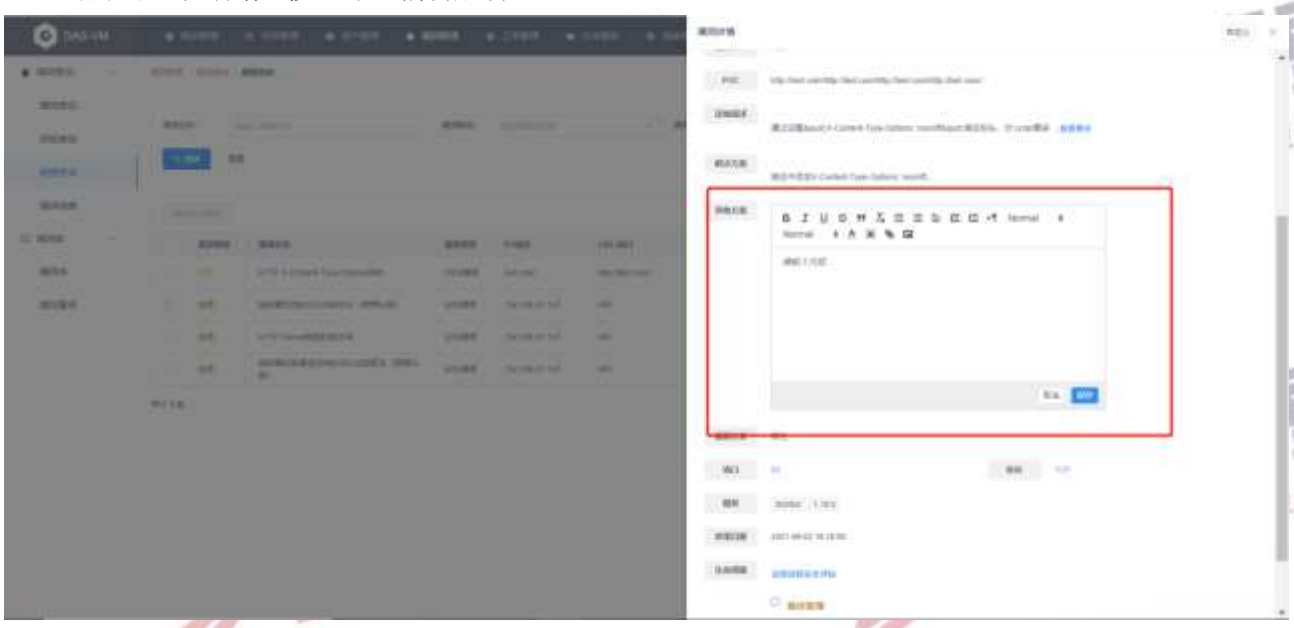
（1） 点击搁置漏洞列表中操作列的<详情>按钮，可以查看对应搁置漏洞的详细信息。



（2） 点击资产相关信息列表中的<查看>按钮，可以查看误报漏洞所属资产的相关详细信息。

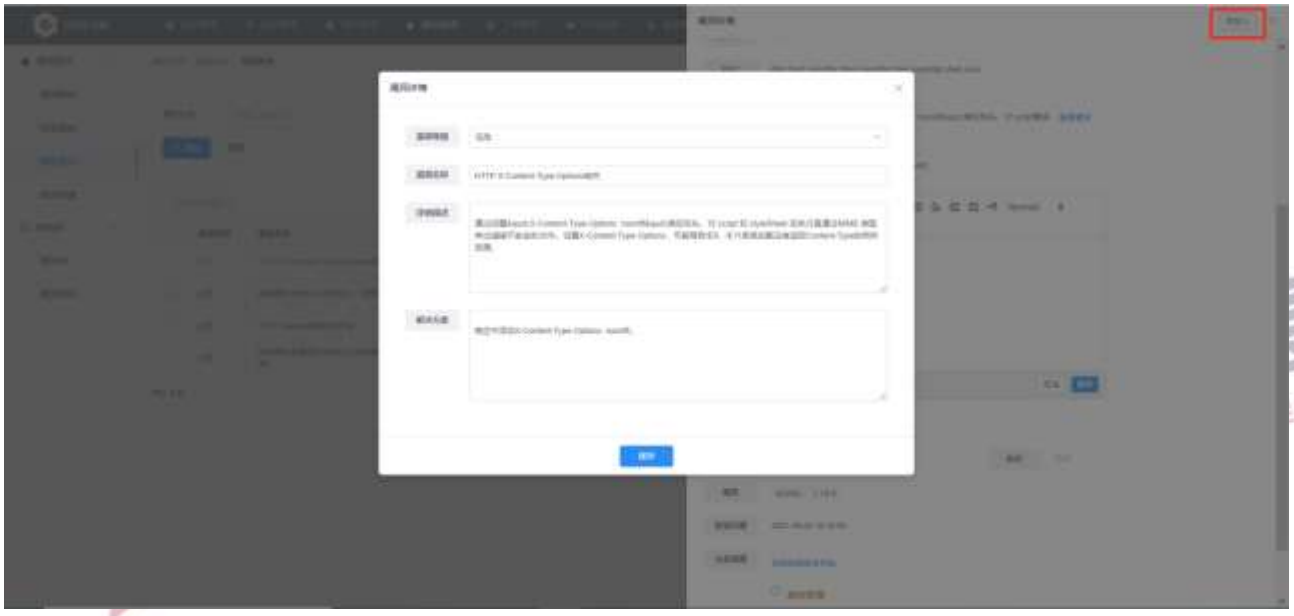


（3） 点击其他方案栏编辑图标可添加或编辑其他解决方案。其他方案栏支持图片和文本形式，编辑完成后点击<保存>按钮即可编辑成功。



6.1.3.3. 漏洞自定义

（1） 点击漏洞详情中的<自定义>按钮，可自定义漏洞等级、漏洞名称、详细描述和解决方案。



6.1.3.4. 取消搁置

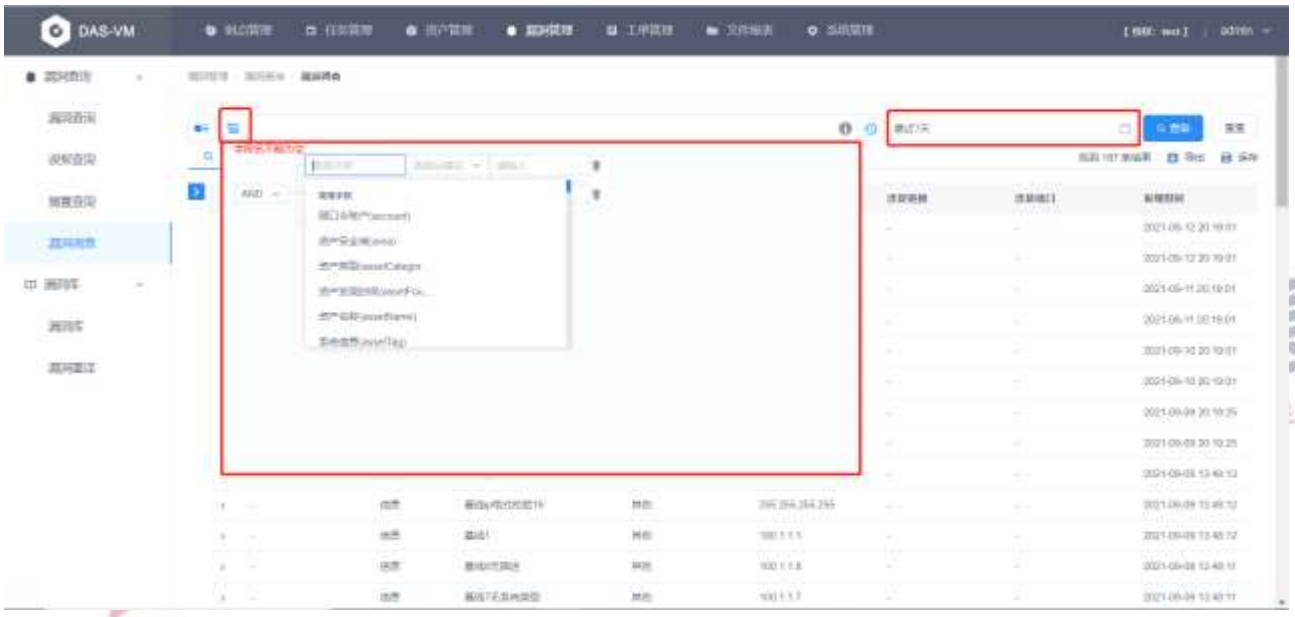
（1） 点击搁置漏洞列表中的<取消搁置>按钮或勾选搁置漏洞点击<批量取消搁置>按钮，可以将选择的漏洞单个或批量取消搁置标记，并从搁置列表中剔除。

6. 1. 4. 漏洞调查

漏洞调查页面主要以历史信息角度，展示所有漏洞入库时的相关详细信息，用户可根据各类灵活的查询条件进行漏洞历史信息查询，漏洞每发现一次，则漏洞调查页面对应增加一条信息。

6.1.4.1. 基础查询

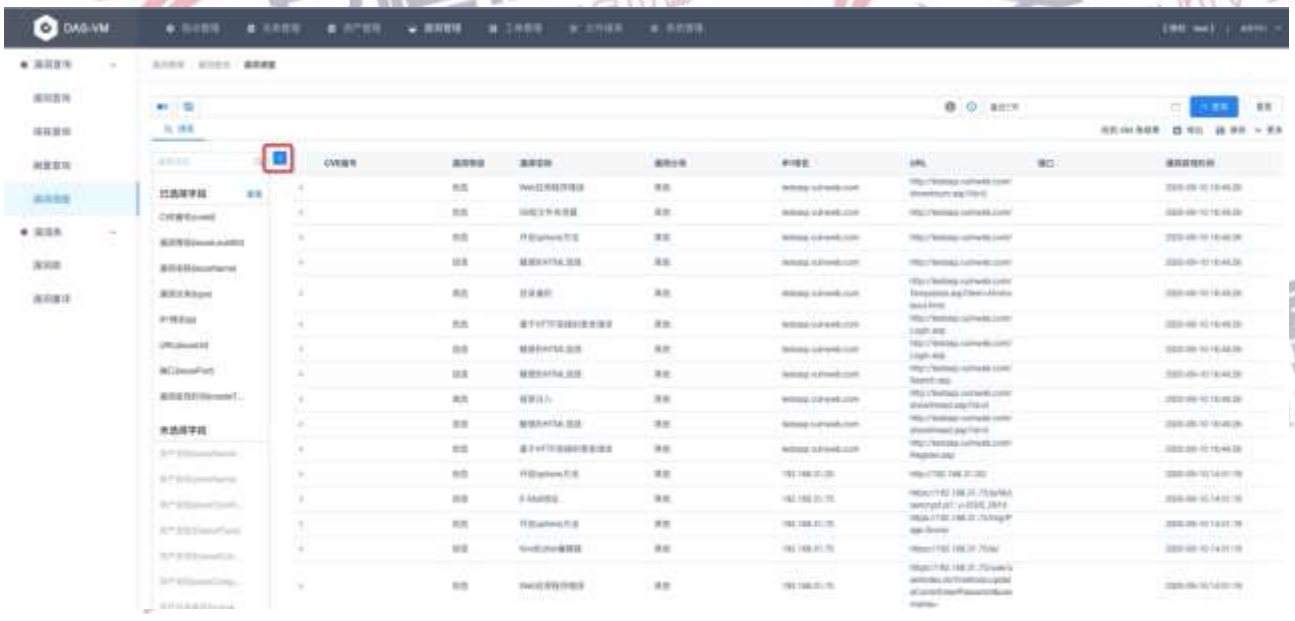
（1） 选择时间、表达式、字段筛选，点击<查询>按钮进行查询。



（2）点击 可以查看搜索语法。

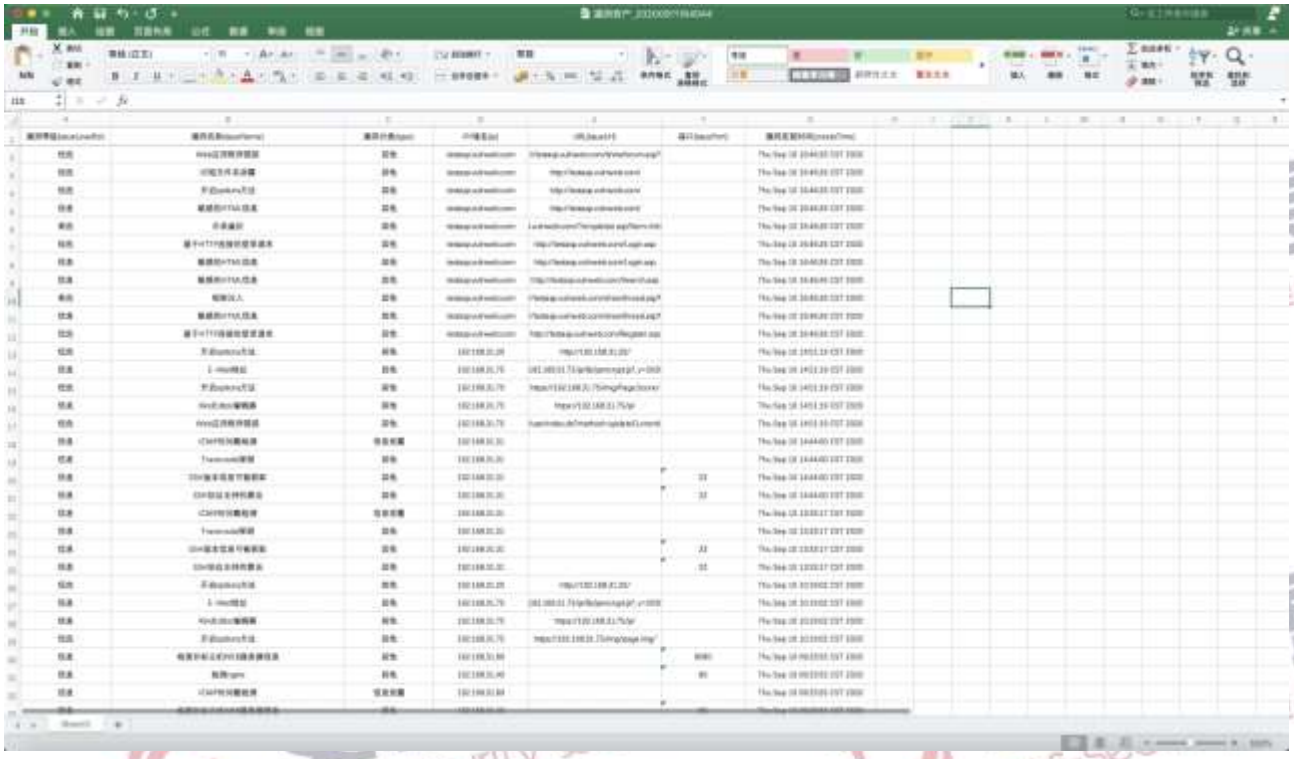
6.1.4.2. 字段显示

（1）点击 按钮重置漏洞显示字段，可选择漏洞列表展示的字段内容。其中，点击已选择字段后面的 号可以删减显示字段，点击未选择字段后的 号可以增加显示字段， 然后点击<重置>按钮，则恢复显示默认字段。



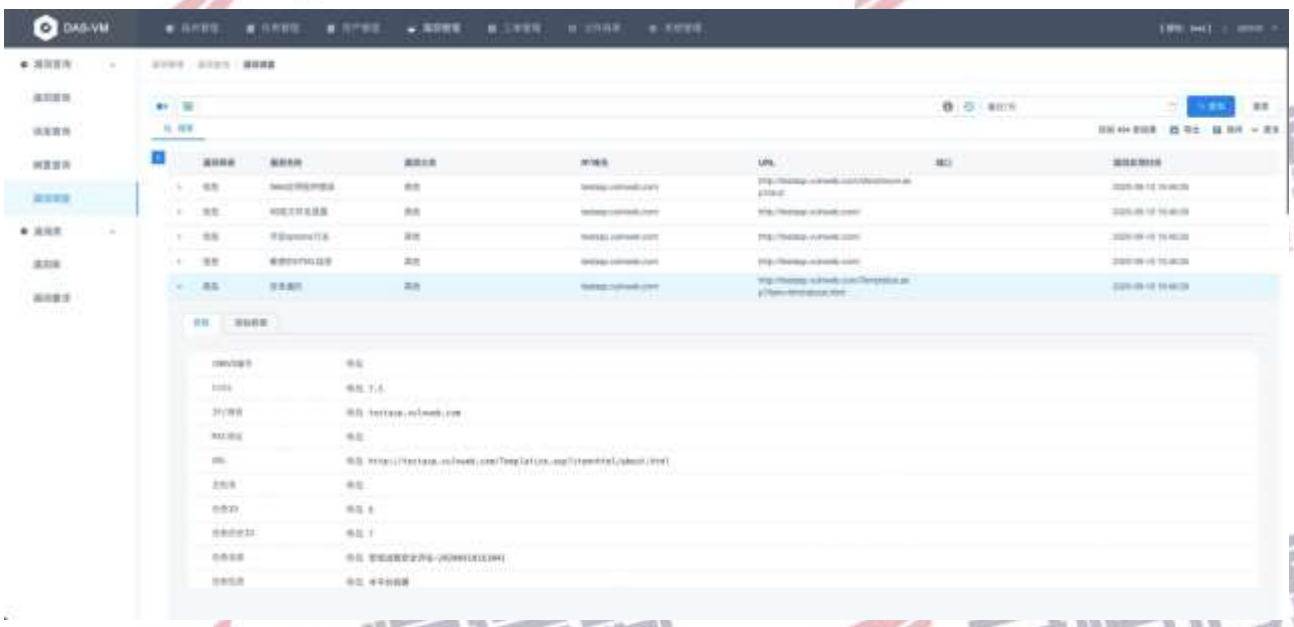
6.1.4.3. 导出

（1） 点击 导出 按钮，可按照列表展示字段格式，导出最近 10000 条漏洞，导出文件格式为 xlsx。



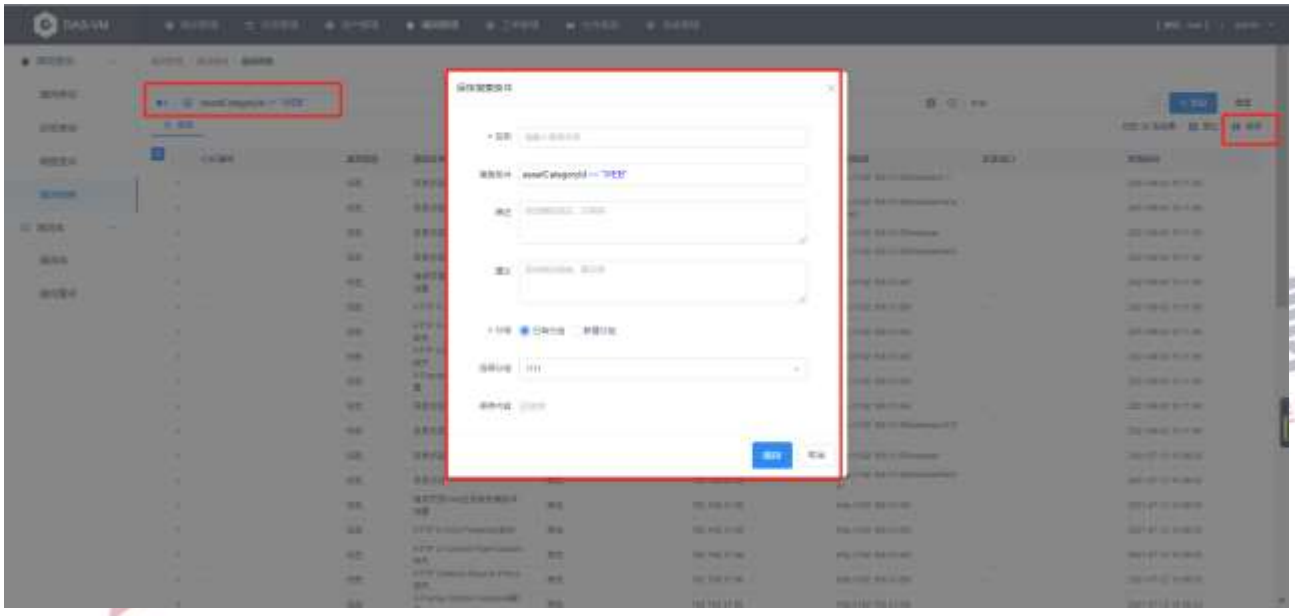
6.1.4.4. 漏洞详情查看

（1） 点击漏洞列表某一漏洞，下拉展示该漏洞的详细全部字段和原始数据。



6.1.4.5. 创建标签

（1） 输入相关查询条件，点击 保存 按钮，填写标签名称并确认，快速标签创建完成。



相关配置参数如下：

配置项	说明
名称	必填项。创建搜索标签的名称。
搜索条件	选填项。可以在基础查询处选择查询项，或者直接输入满足格式要求的搜索条件。
描述	选填项。创建搜索标签的描述。
建议	选填项。创建搜索标签的建议。
分组	必填项。创建搜索标签的分组，可以选择已有分组和新建分组。
选择/新建分组	选填项，选择已经创建好的分组，或者新建分组。
保存内容	默认为开启搜索。

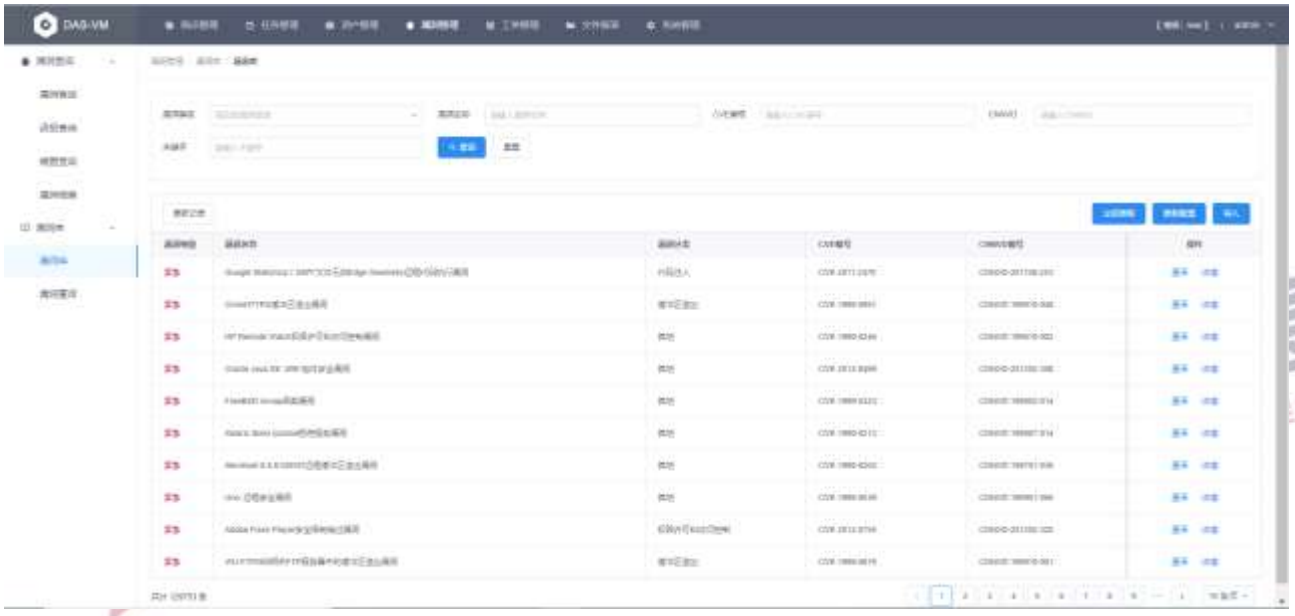
6.2. 漏洞查询

6. 2. 1. 漏洞库

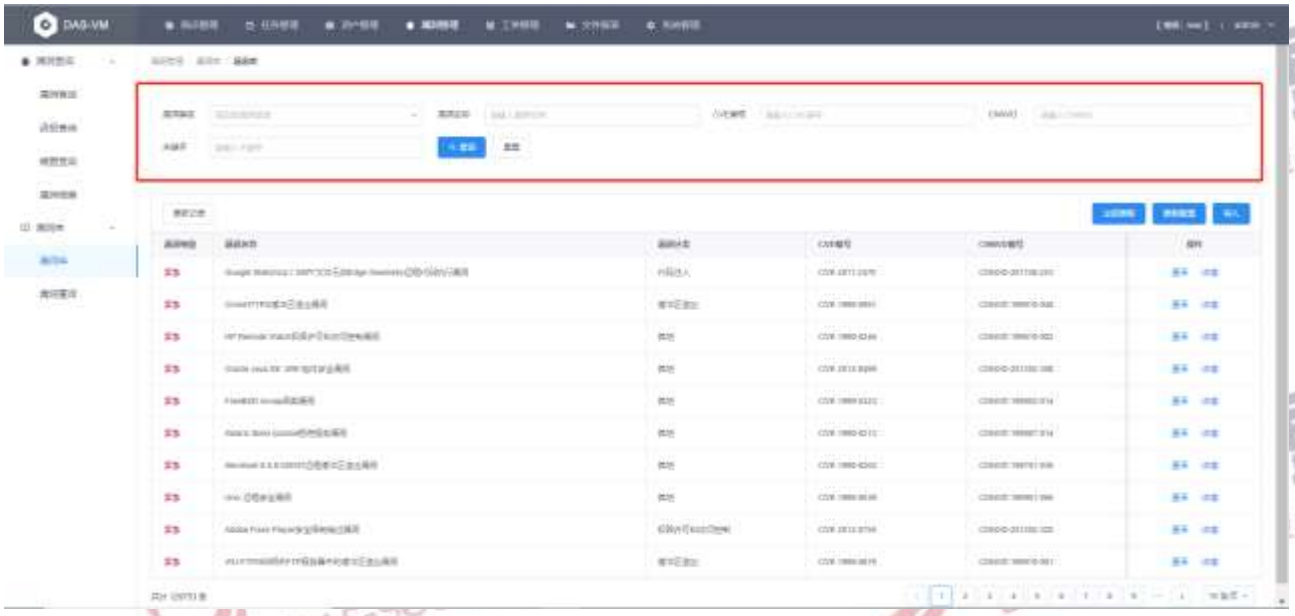
漏洞库中存储着各类重要漏洞积累，以及扫描出的新增类型漏洞均会保存在漏洞库中。

6. 2. 1. 1. 漏洞库查询

（1） 用户 WEB 登录后，进入[漏洞管理 /漏洞库 /漏洞库]页面。

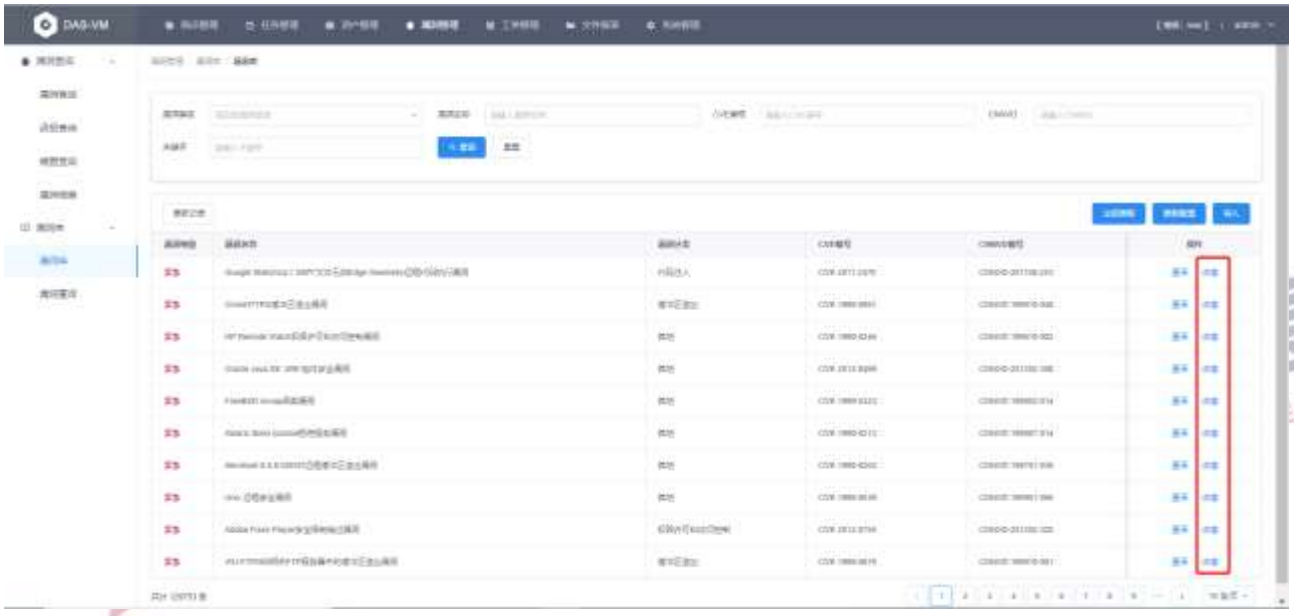


（2）设置查询条件，可在漏洞库中进行指定漏洞查询，条件设置后，点击<查询>按钮，进行查询。

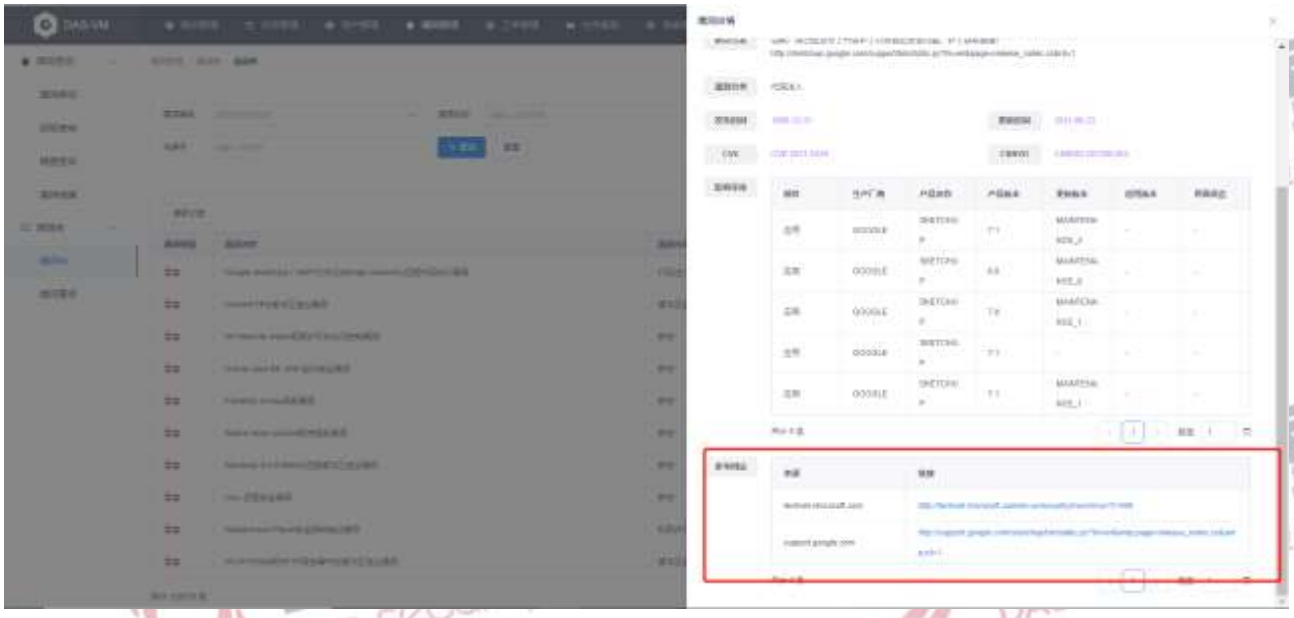


6. 2. 1. 2. 漏洞详情

（1）点击漏洞列表中的<详情>按钮，可以查看对应漏洞的漏洞等级、漏洞名称、详细描述和解决方案等信息。



（2） 点击参考网址的具体链接可以查看对应漏洞来源的更多详细信息。

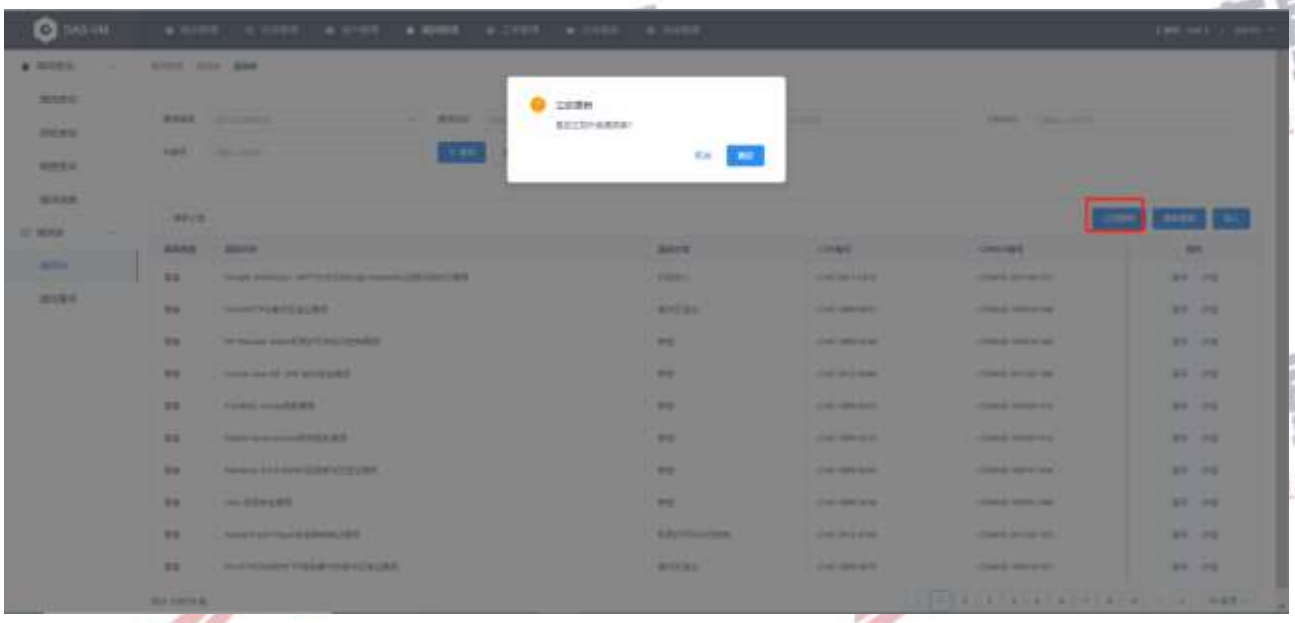


6. 2. 1. 3. 漏洞重译

（1） 点击漏洞列表中的<重译>按钮，编辑漏洞名称、详细描述、解决方案，点击<保存>按钮，可以自定义漏洞的漏洞等级、漏洞名称、详细描述、解决方案四个字段信息。

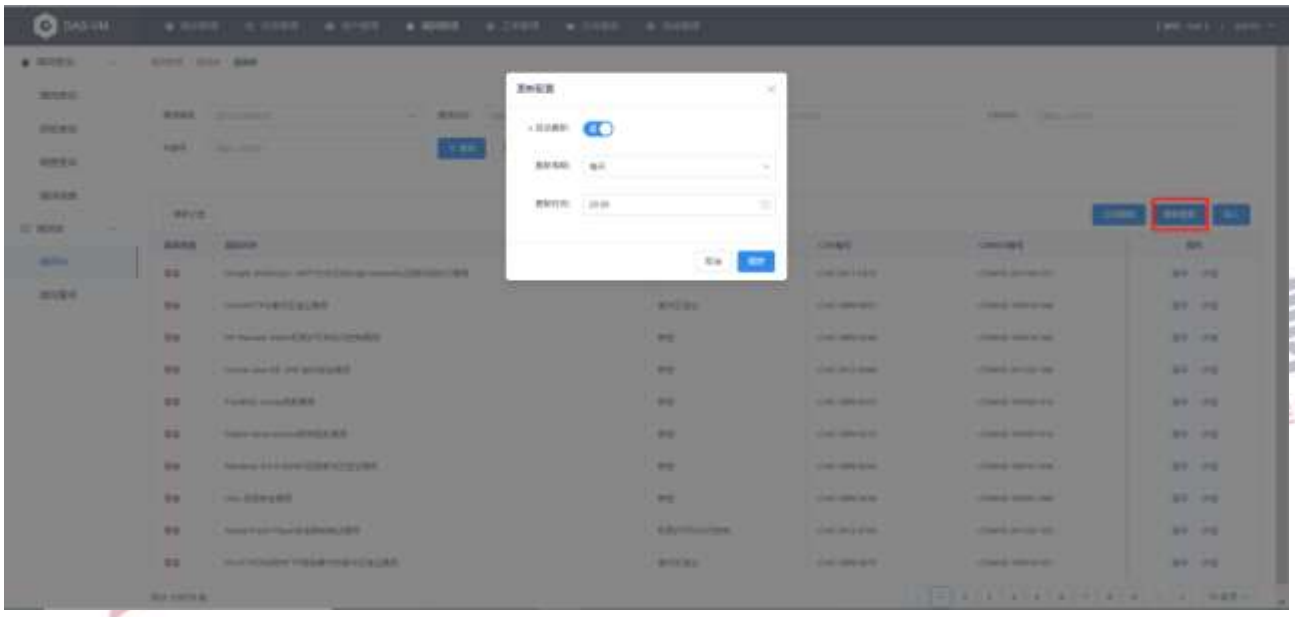
6.2.1.4. 漏洞库更新

（1） 点击<立即更新>按钮，确认是否立即更新。



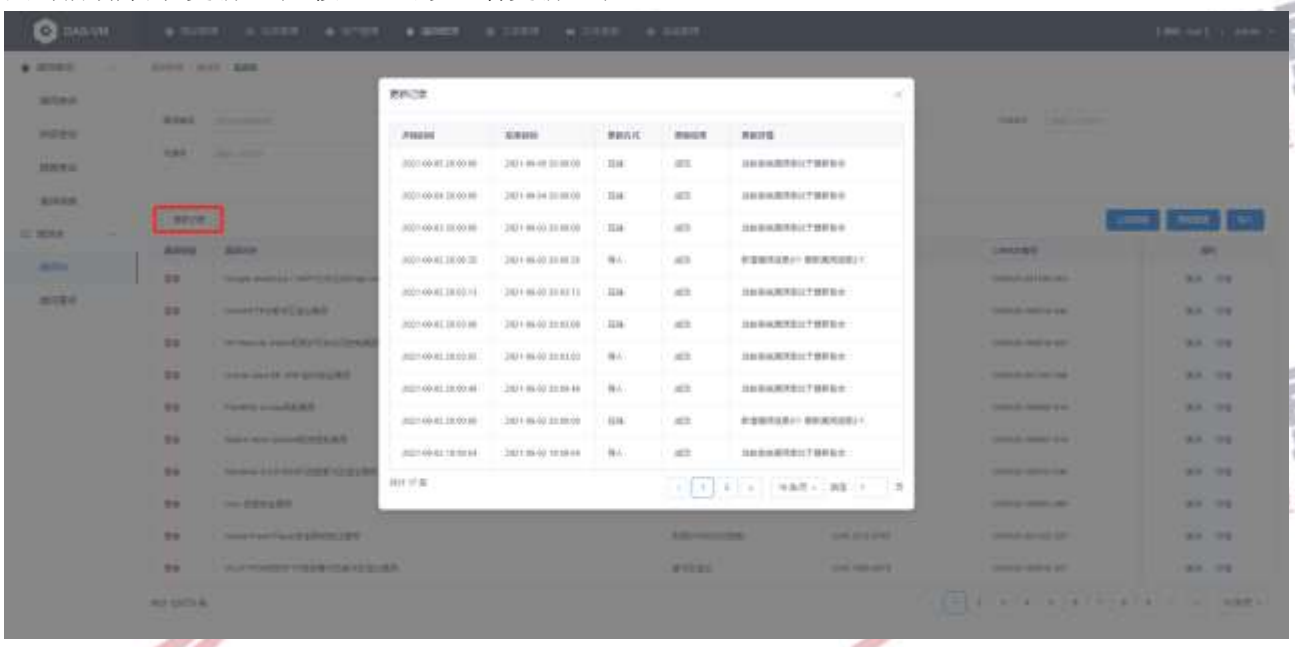
6.2.1.5. 漏洞库更新配置

（1） 点击<更新配置>按钮，可以选是否自动更新。开启自动更新后，可以选择更新周期、更新时间。



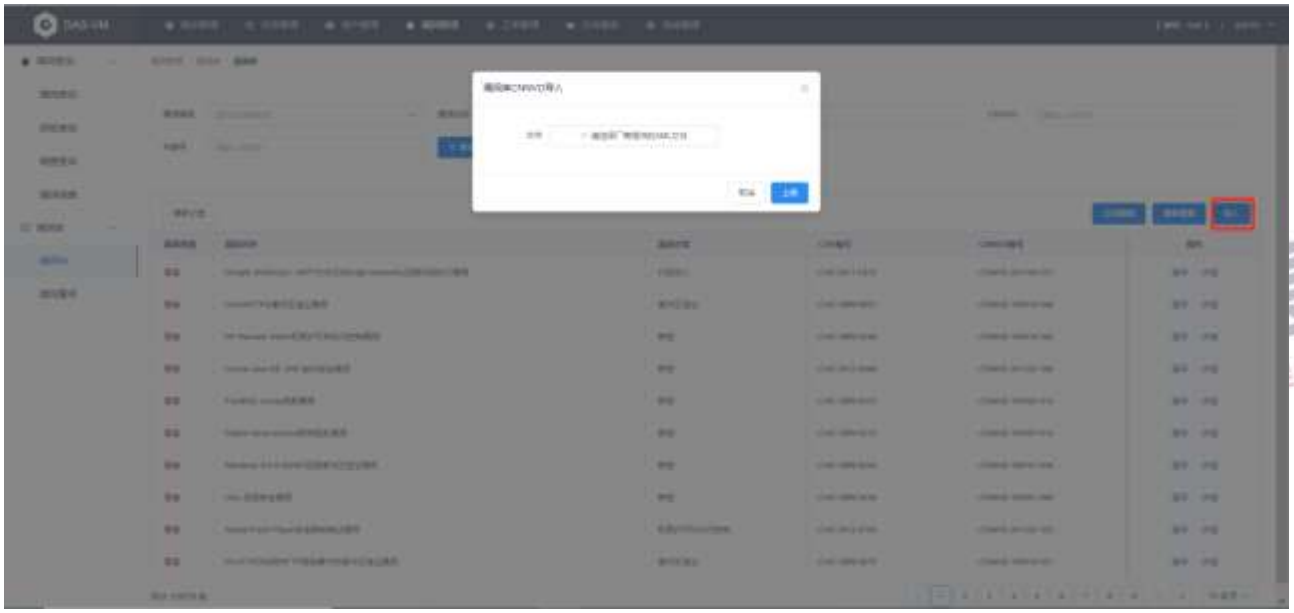
6.2.1.6. 漏洞库更新记录

（1） 点击漏洞库的<更新记录>按钮，可以查看更新记录。



6.2.1.7. 漏洞库导入

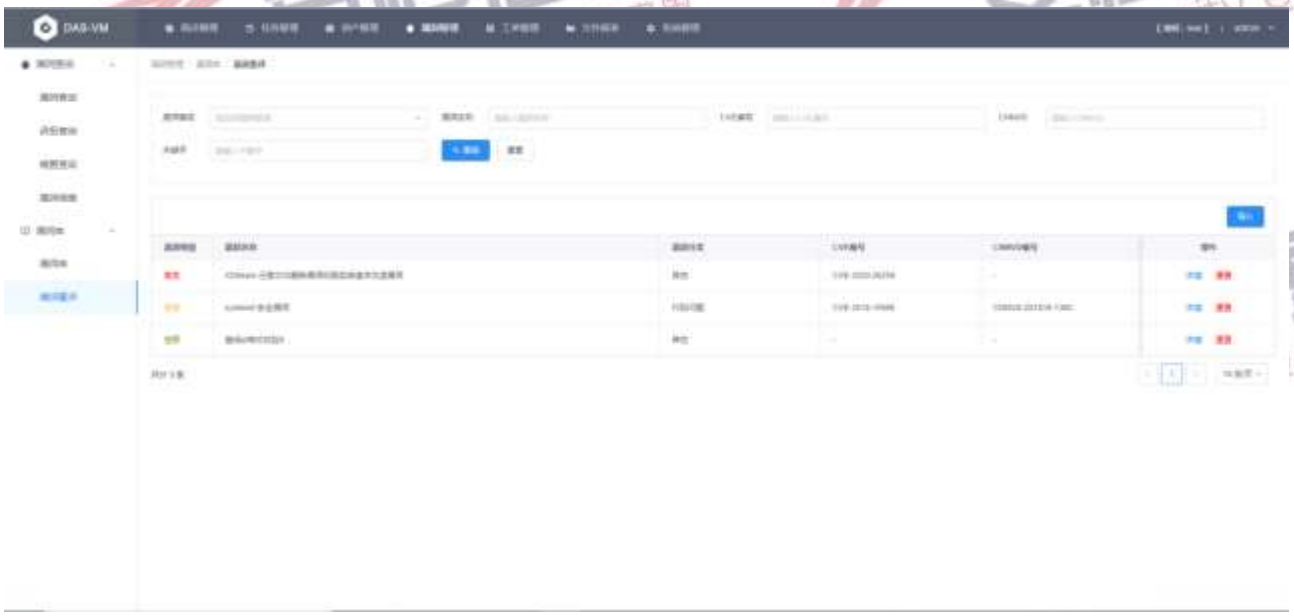
（1） 点击<导入>按钮，选择厂商提供的 xml 文件，点击<上传>按钮上传漏洞库漏洞。



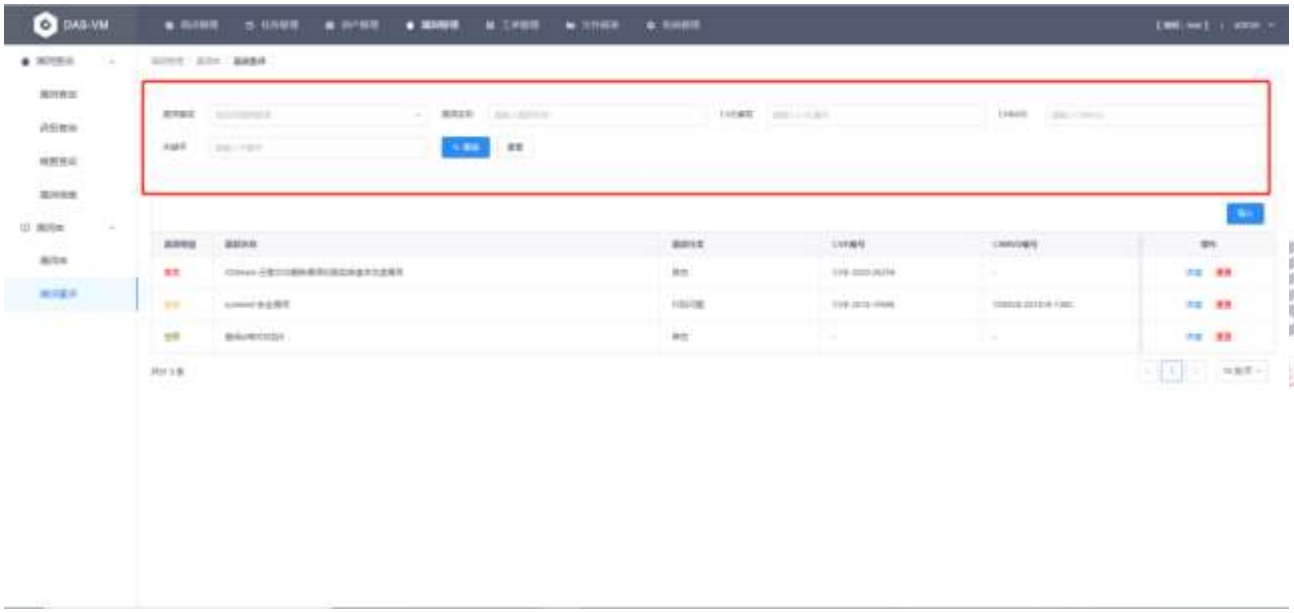
6.2.2. 漏洞重译

6.2.2.1. 重译漏洞查询

（1） 用户 WEB 登录后，进入[漏洞管理 /漏洞库 /漏洞重译]页面。

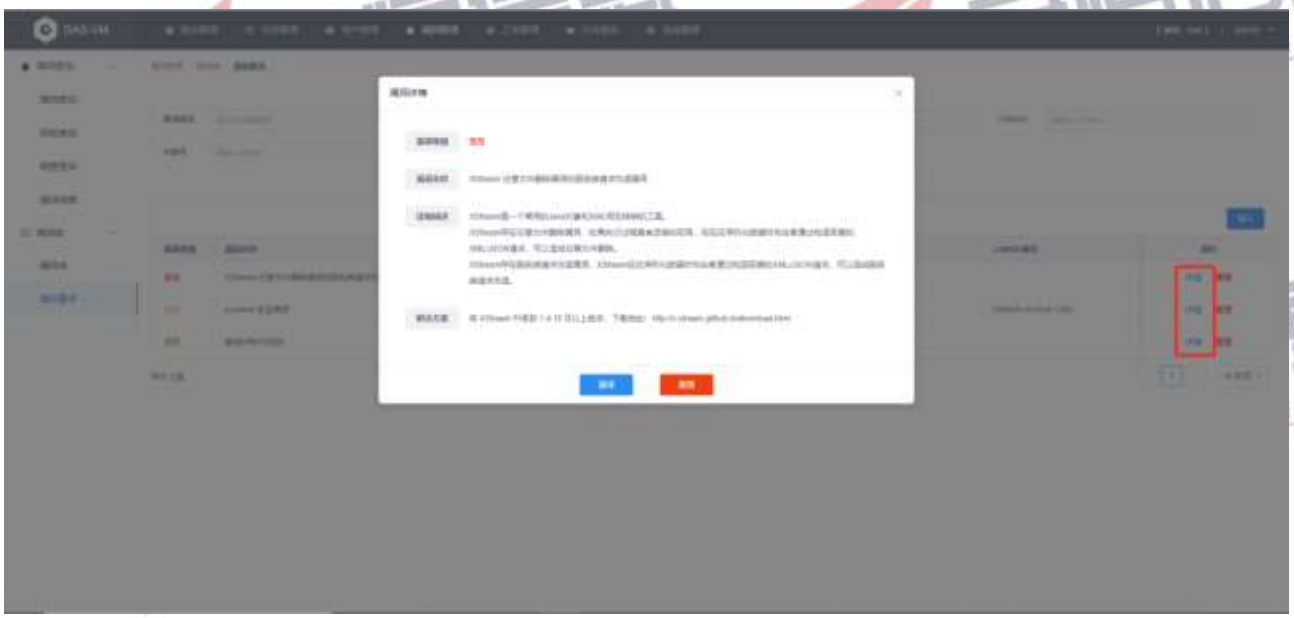


（2） 设置查询条件，可在漏洞库中进行指定漏洞查询，条件设置后，点击<查询>按钮，进行查询。



6.2.2.2. 漏洞详情

（1） 点击漏洞列表中的<详情>按钮，可以查看对应漏洞的详细信息。

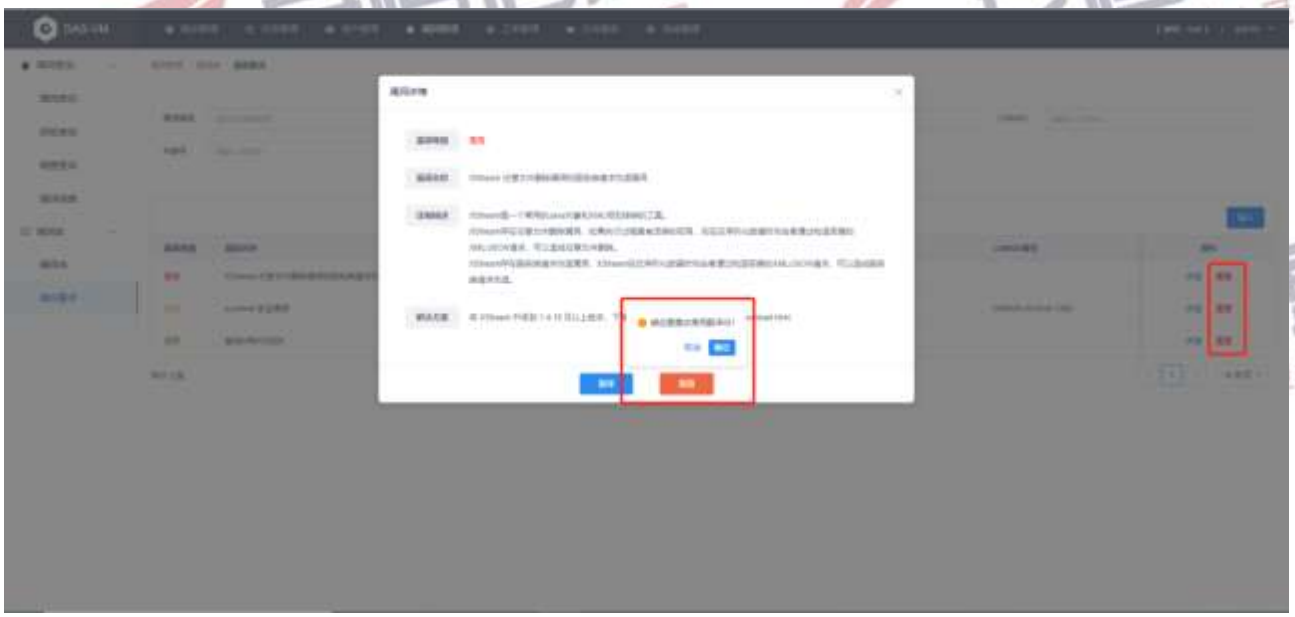


6.2.2.3. 漏洞重译

（1） 点击漏洞详情下方的<重译>按钮，编辑漏洞等级、漏洞名称、详细描述、解决方案，点击<保存>按钮，可以自定义漏洞的漏洞等级、漏洞名称、详细描述、解决方案四个字段信息。

6.2.2.4. 漏洞重置

（1） 点击漏洞列表中的<重置>按钮或漏洞详情下方的<重置>按钮并确认，可以取消漏洞重译，恢复漏洞默认漏洞等级、漏洞名称、详细描述、解决方案，并从漏洞重译漏洞列表中剔除。



7. 工单管理

7.1. 工单管理

7.1.1. 公告下发

将公告下发给全部责任人，一般用于中高危漏洞的公告下发。

7.1.1.1. 公告新增

（1） 用户 WEB 登录后，进入[工单管理 /工单管理/公告下发]页面。

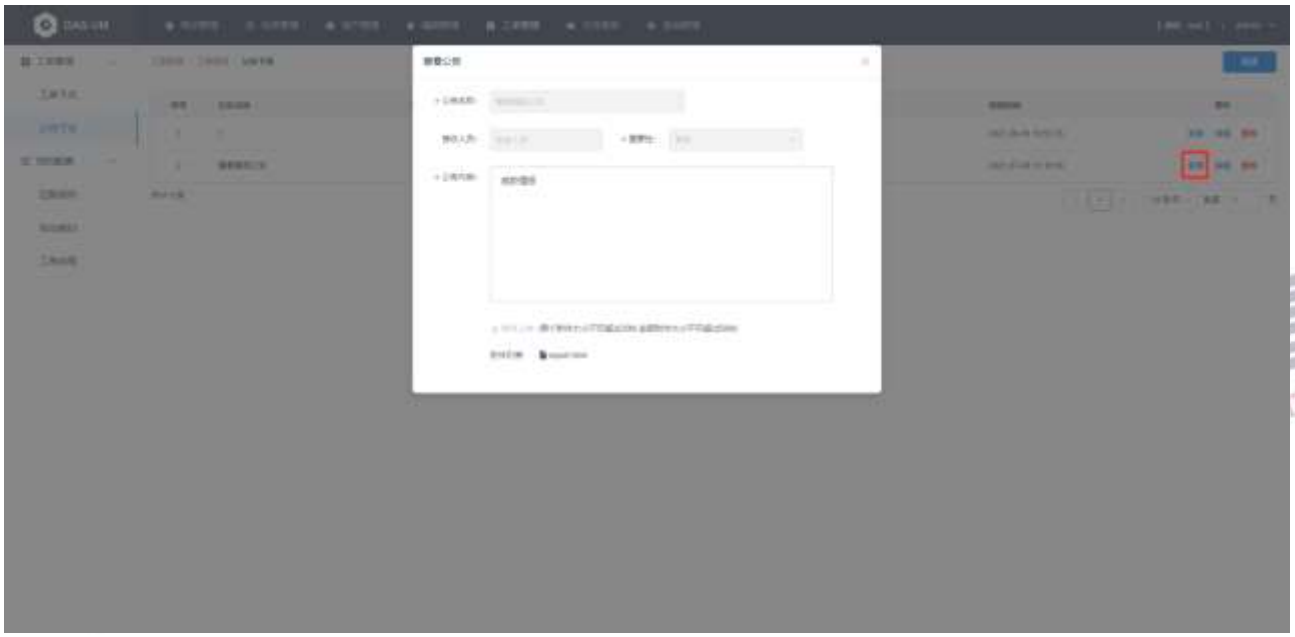
（2）点击<新建>按钮，在弹出的新增公告窗口，填写公告名称、公告内容等相关信息，选择重要性，还可上传相应附件，点击<保存>按钮即可新增一条公告，公告内容支持图片、文本形式。

注意

单个附件大小不可超过 20M,全部附件大小不可超过 50M

7.1.1.2. 公告查看

（1） 点击公告列表操作列的<查看>按钮，在弹出的相应公告查看窗口，可以查看公告的详细信息。

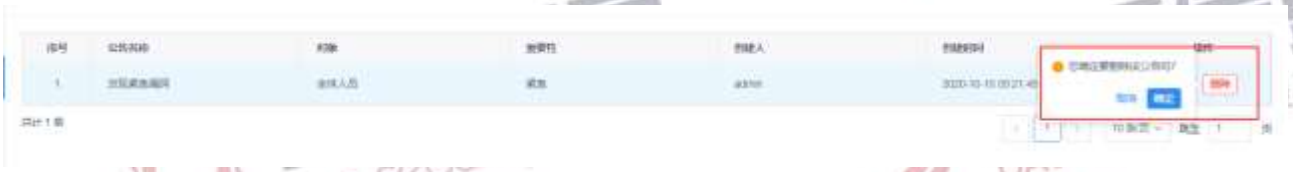


7.1.1.3. 公告编辑

（1） 点击公告列表操作列的<编辑>按钮，在弹出的相应公告编辑窗口，编辑公告名称、公告内容、重要性、附件等相关信息，点击<保存>按钮即可编辑成功。

7.1.1.4. 公告删除

（1） 点击公告列表操作列的<删除>按钮，在弹出的删除公告确认窗口，点击<确定>按钮，即可删除相应公告。



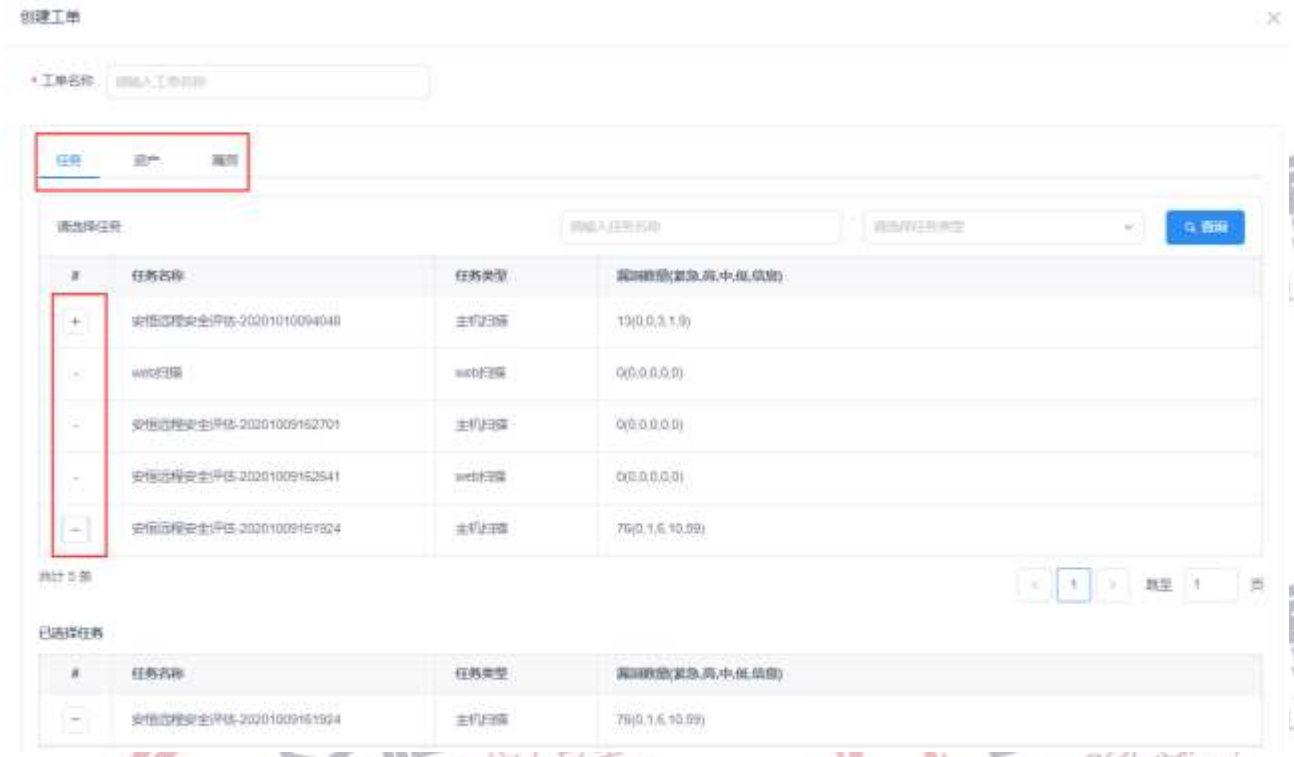
7.1.2. 工单下发

7.1.2.1. 创建工单

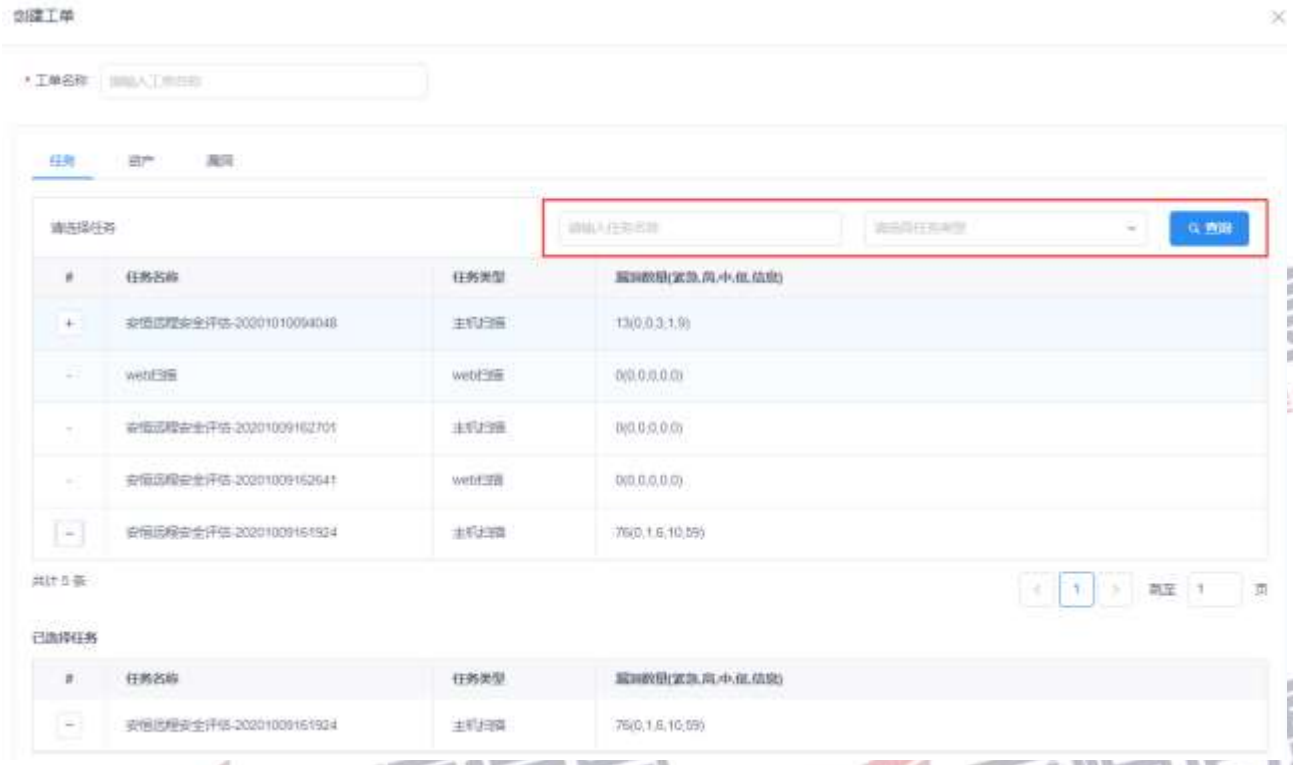
（1） 用户 WEB 登录后，进入[工单管理 /工单管理/工单下发]页面。

（2） 点击<创建工单>按钮，弹出创建工单窗口。

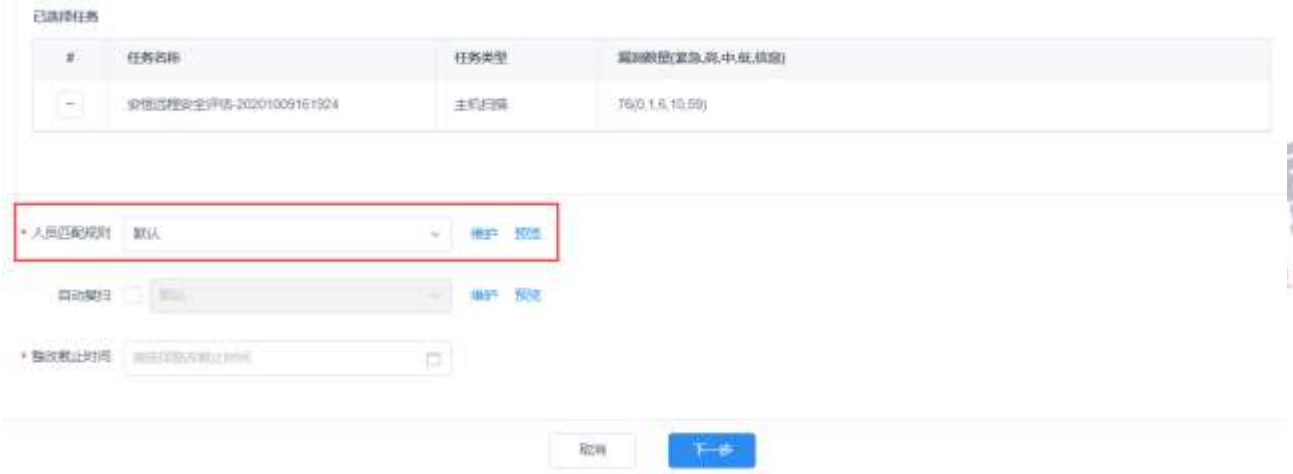
（3） 填写工单名称，选择漏洞。支持按任务、资漏洞方式进行漏洞的过滤选择漏洞，点击可切换过滤方式，过滤方式只能选择一种；点击目标列表前“+”或“—”图标选择或取消选择目标，可选择多个派单目标。



（4） 任务列表包括扫描任务列表和渗透测试任务列表，资产列表包括主机资产列表和应用资产列表设置查询条件，点击<查询>按钮可查询指定任务/资产/漏洞。



（5）选择对应的人员匹配规则，系统默认出厂规则为按资产责任人匹配。点击<维护>按钮可新增窗口并进入[工单管理/规则配置/匹配规则]页面进行匹配规则编辑，点击<预览>按钮可查看所选人员匹配规则的详细内容。

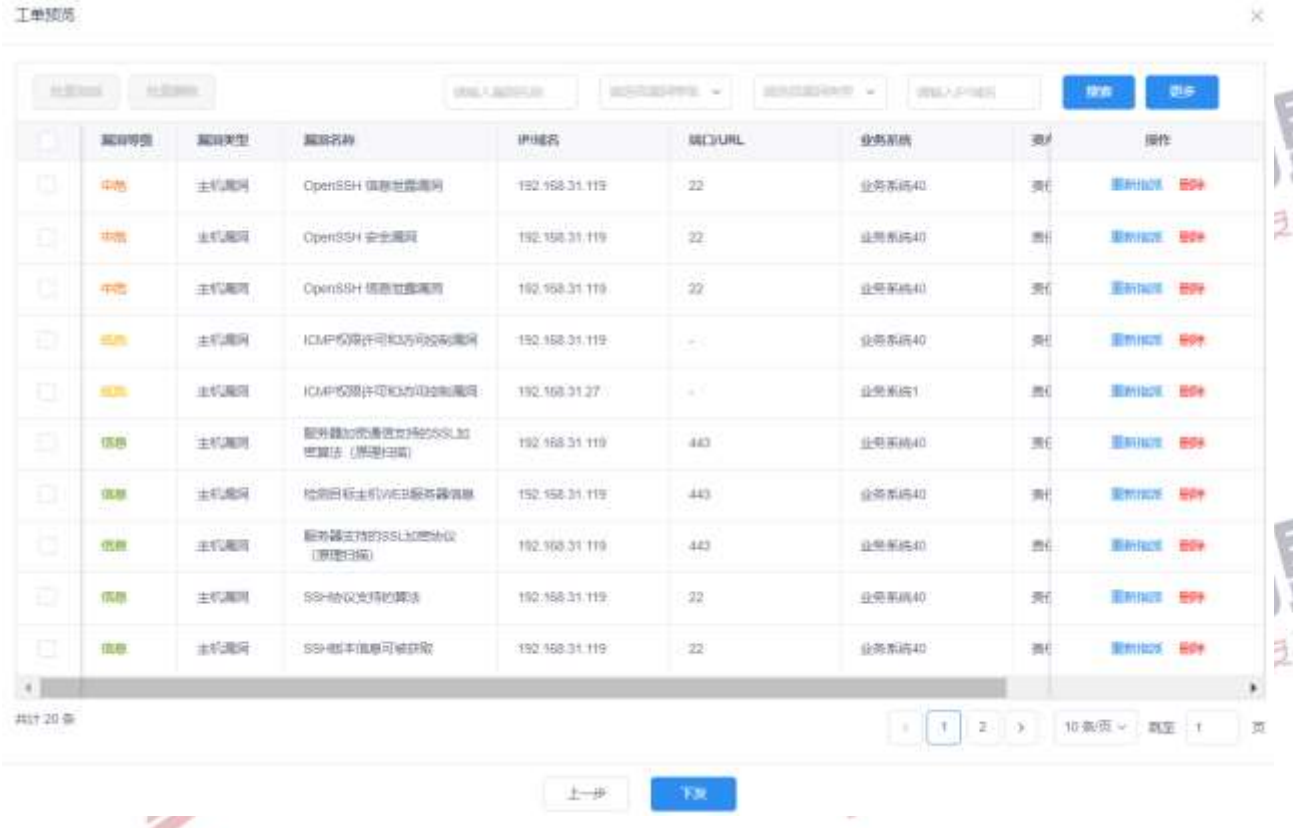


（6）选择是否启动自动复扫，若启动自动复扫需勾选自动复扫并选择对应的自动复扫规则，系统默认出厂规则为当中危漏洞数大于等于 20 个时发起自动复扫。点击<维护>按钮可新增窗口并进入[工单管理 /规则配置/自动复扫]页面进行自动复扫规则编辑，点击<预览>按钮可查看所选自动复扫规则的详细内容。

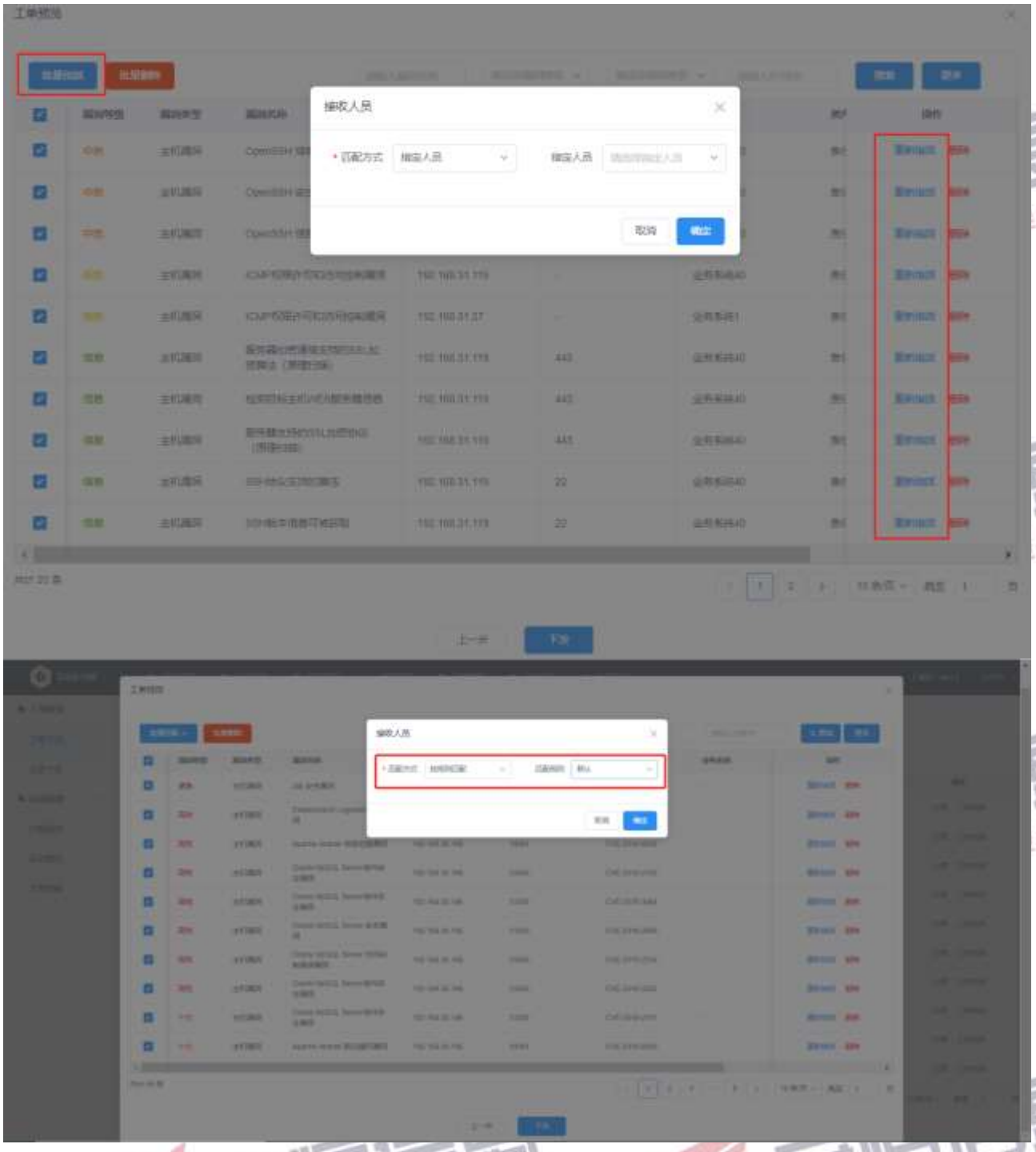
（7） 选择对应的整改截止时间，点击<下一步>按钮完成工单创建，自动按所选人员匹配规则进行漏洞责任人匹配，进入**工单预览**界面。若人员匹配规则为不派单的将自动从工单中剔除。

7.1.2.2. 工单下发管理

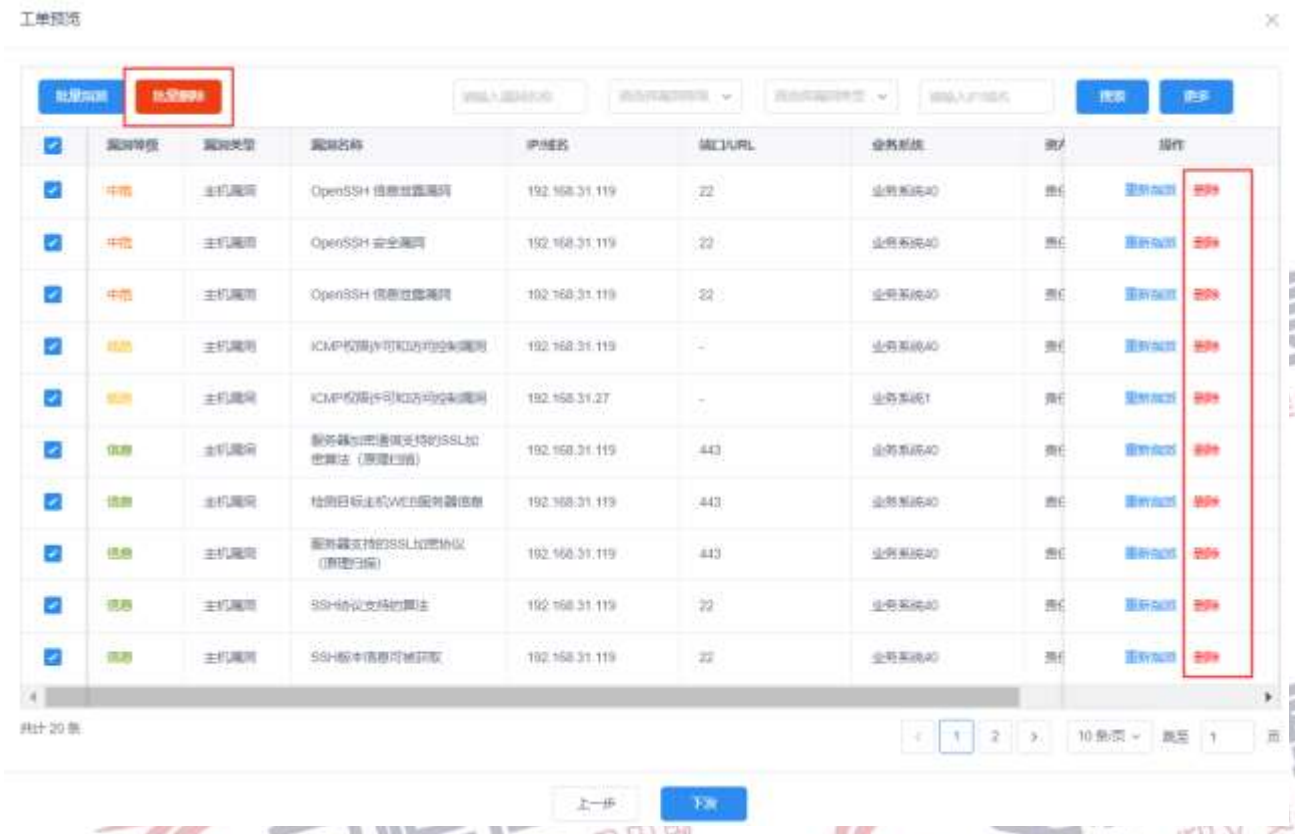
（1） 工单预览页面可以查看当前即将下发的漏洞列表，横向滚动可查看漏洞相关业务系统、资产责任人、漏洞匹配责任人信息。



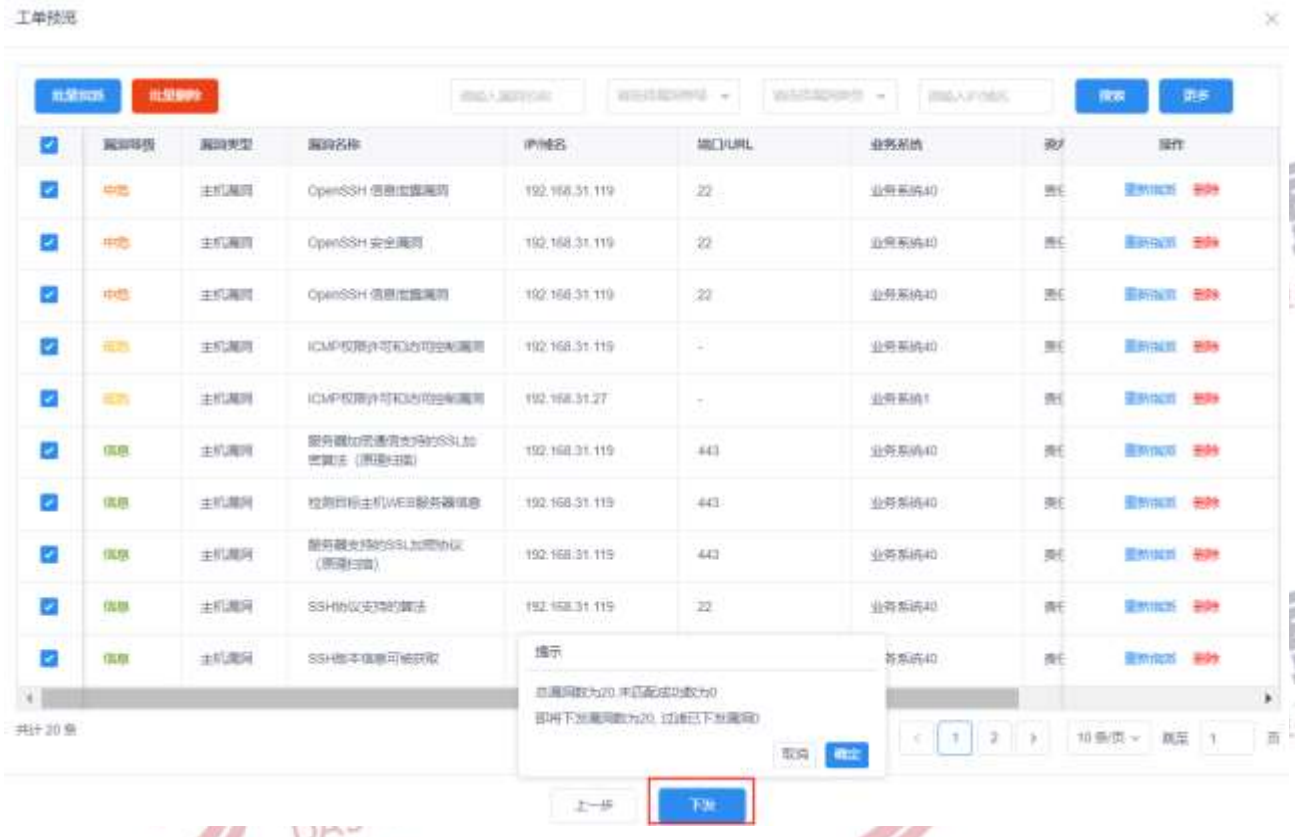
（2）当漏洞责任人不符合预期时，可点击<重新指派>按钮或勾选多个漏洞点击<批量指派>按钮选择匹配方式，点击<确定>按钮重新匹配漏洞责任人。当匹配方式为指定人员时需选择指定人员；同时匹配方式支持按规则匹配，并选择匹配规则。



（3）当列表中存在不需要下发的漏洞时，可点击<删除>按钮或勾选多个漏洞点击<批量删除>按钮并确认进行漏洞删除。删除后漏洞将从预览列表中移除，本次下发将不再包含该漏洞，该漏洞可在后续新建工单时重新选择并下发。

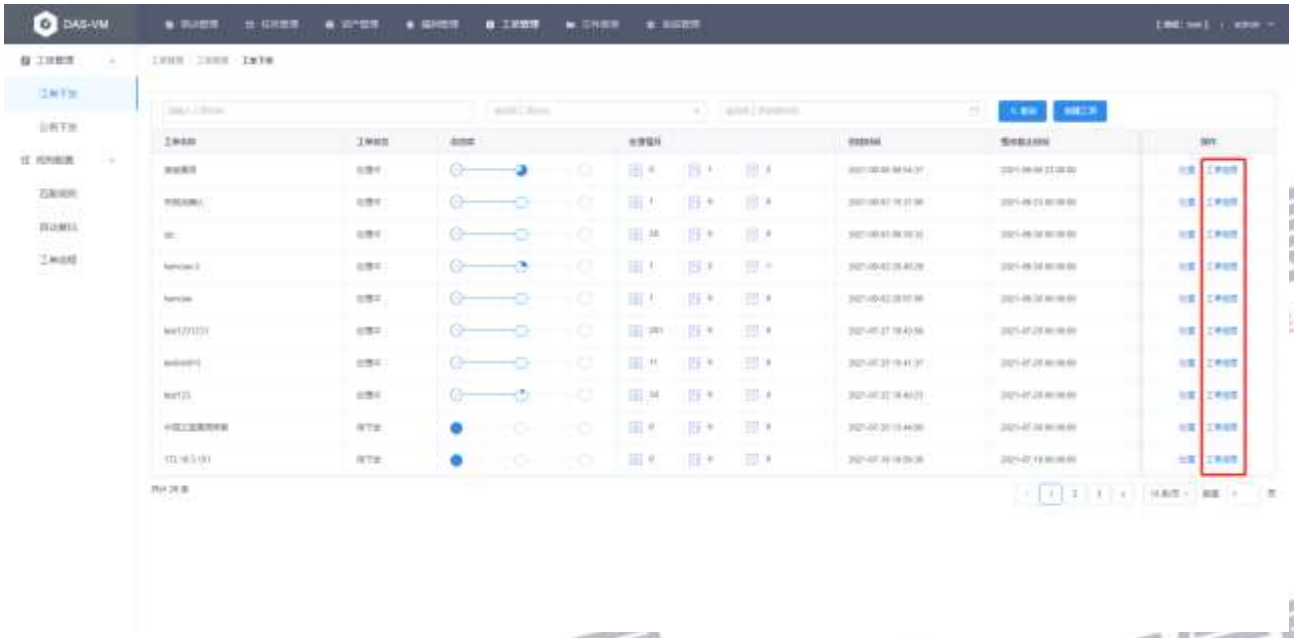


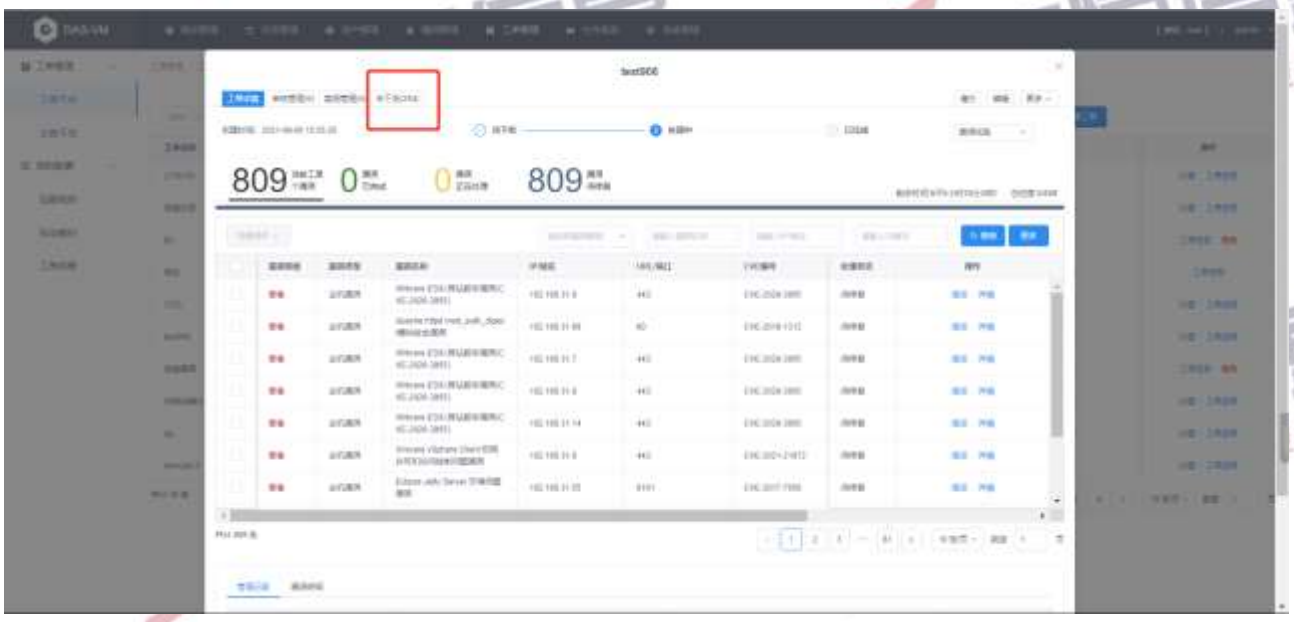
（4） 点击<下发>按钮，本次所有漏洞将下发给对应的漏洞责任人

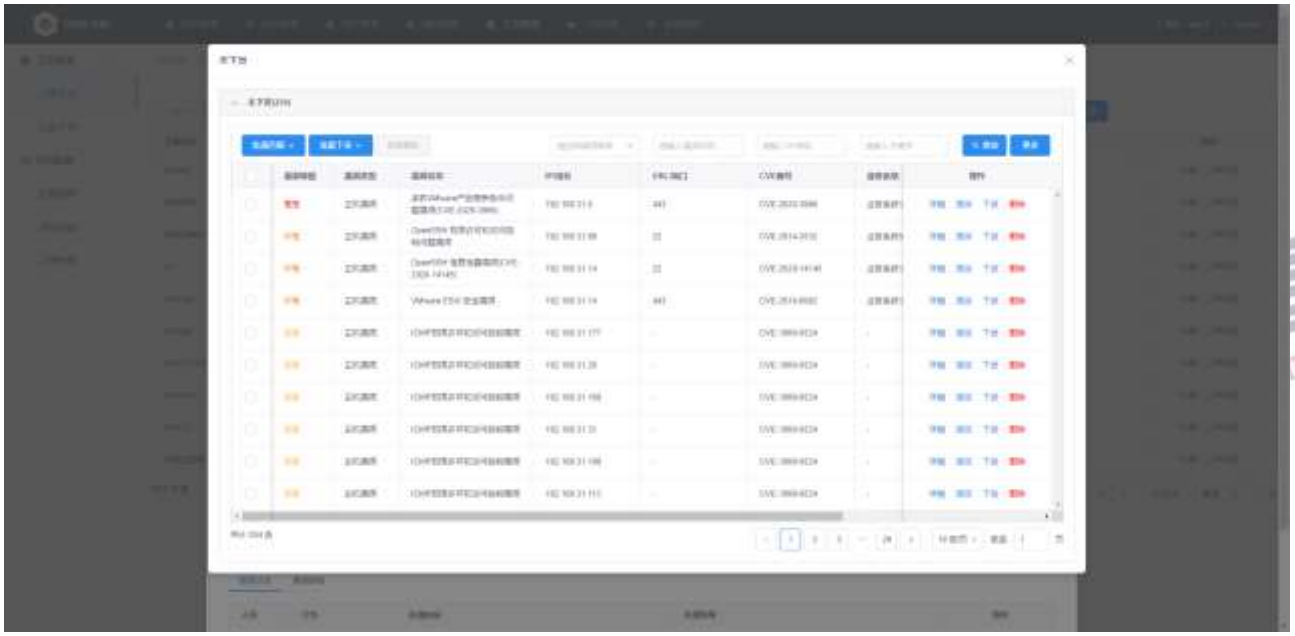


（5） 当存在漏洞责任人为空的漏洞时，该漏洞将无法正确下发至漏洞责任人，下发时漏洞将自动转移至该工单的“**未下发**”列表中。可点击工单列表的<工单信息>按钮，展开工单信息详情，点击<

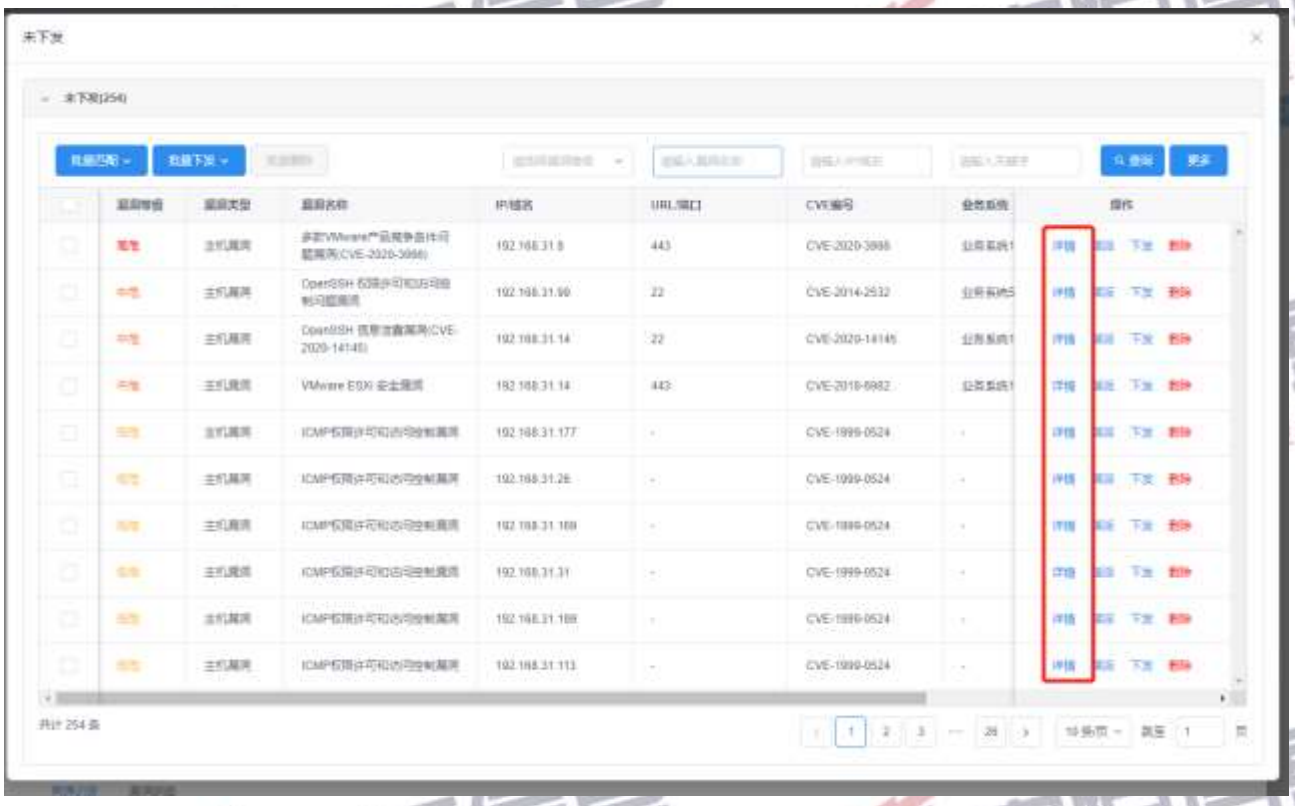
未下发>进入未下发页面查看未下发漏洞列表。横向滚动可查看漏洞相关业务系统、资产责任人、漏洞匹配责任人信息。

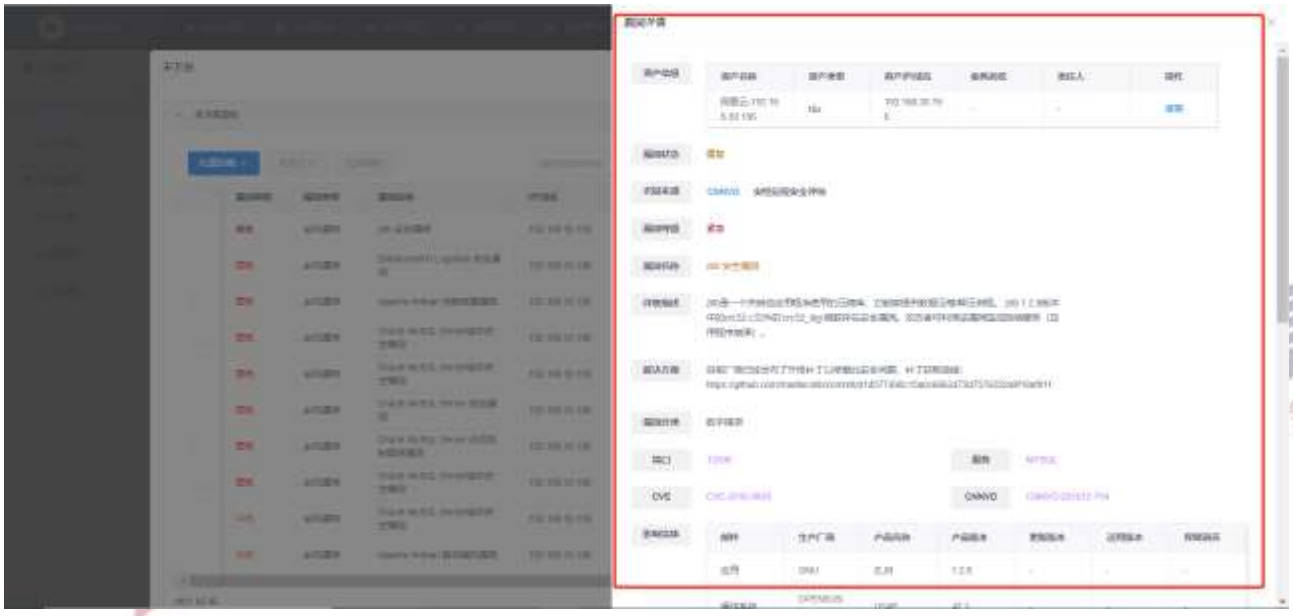




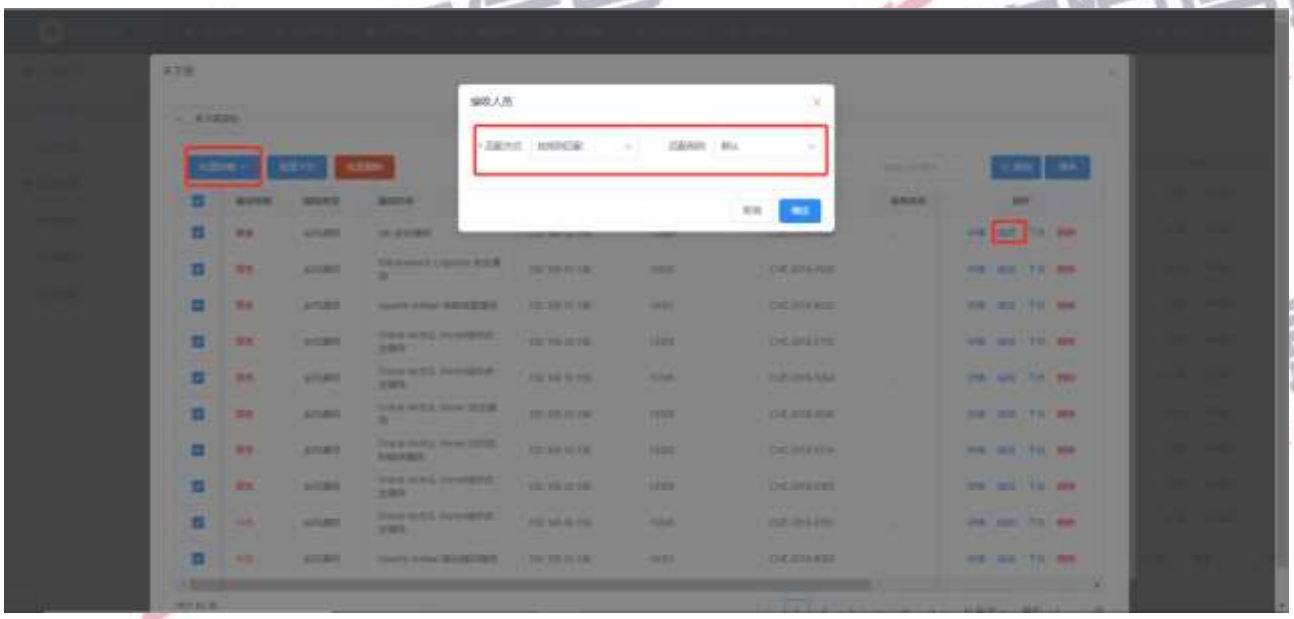


（6）点击漏洞列表<详情>按钮可查看漏洞的详细信息。

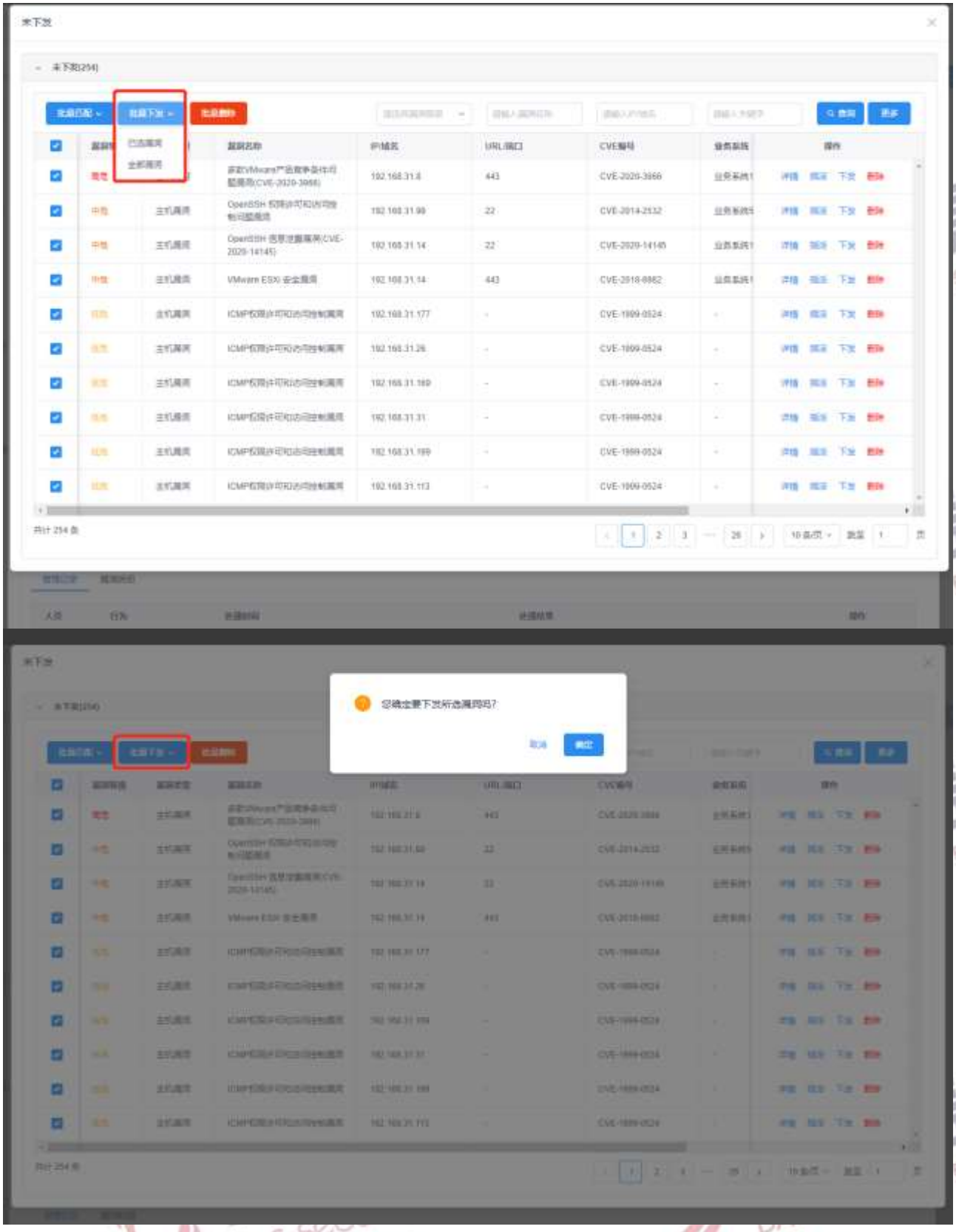




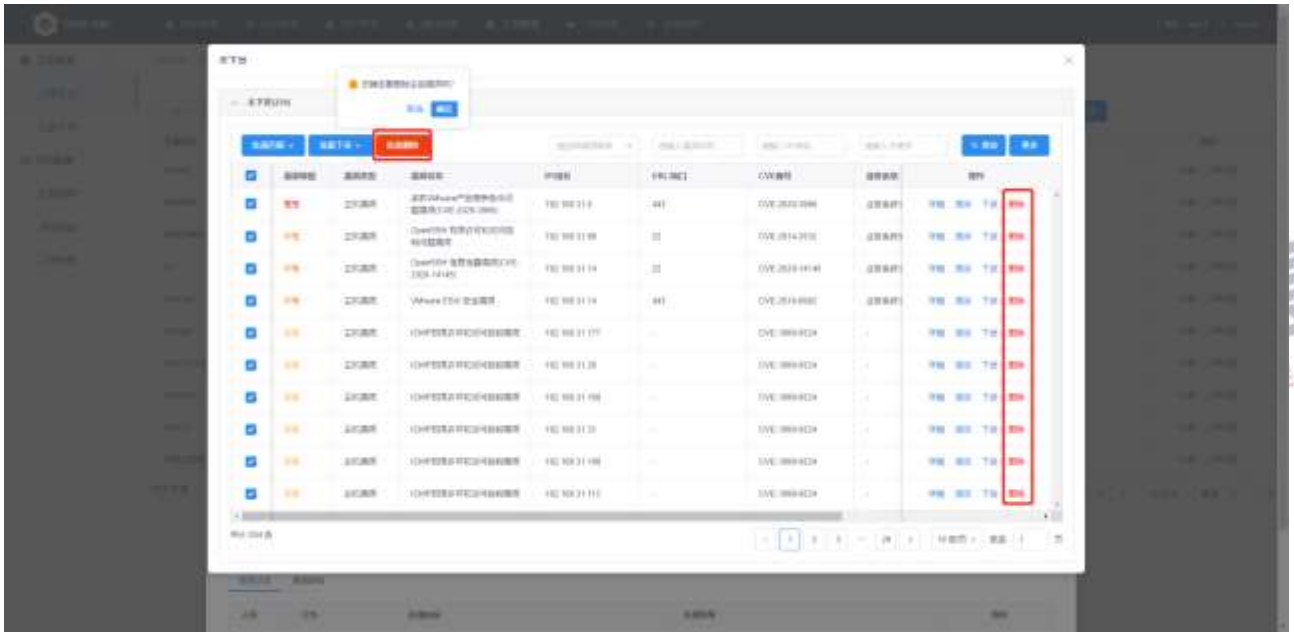
（7） 勾选漏洞点击<批量匹配>按钮重新选择匹配方式，已选漏洞或者全部漏洞，点击<确定>按钮重新匹配漏洞责任人。当匹配方式为指定人员时需选择指定人员；同时也支持规则匹配，并且需要选择规则匹配方式。



（8） 重新匹配漏洞责任人后，可勾选漏洞点击<批量下发>按钮，选择已选漏洞或者全部漏洞，然后并确认，将漏洞下发给对应的漏洞责任人。



（9）当列表中存在不需要下发的漏洞时，可点击<删除>按钮或勾选漏洞点击<批量删除>按钮并确认可删除。删除后漏洞将从该工单中移除，该漏洞可在后续新建工单时重新选择并下发。



7.1.2.3. 工单查询

（1） 设置查询条件，可在工单管理列表中进行指定工单查询，条件设置后，点击<查询>按钮，进行查询。

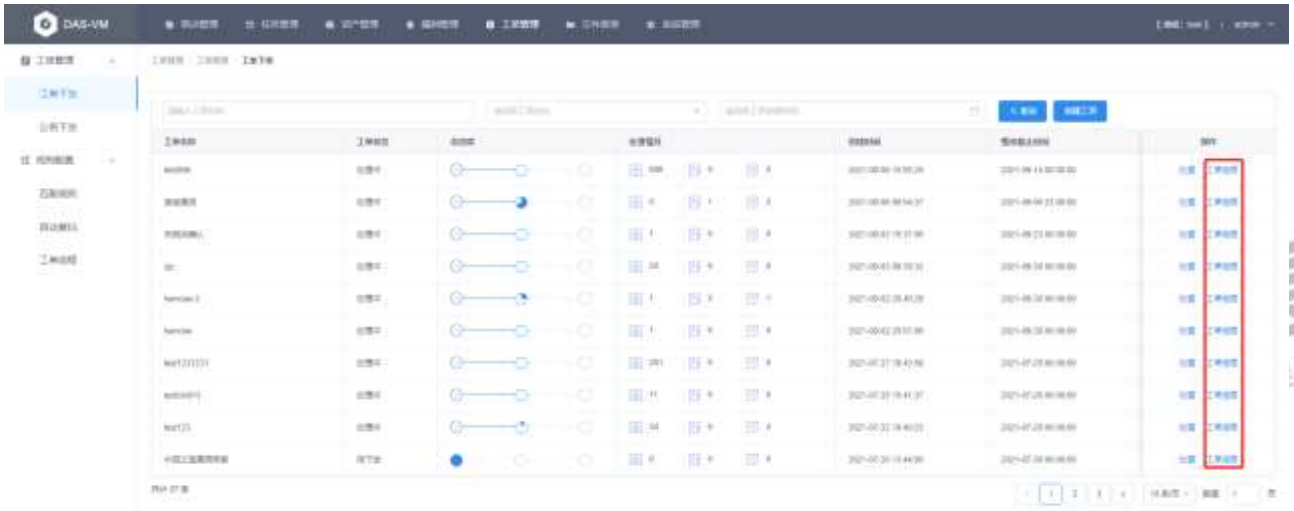
（2） 工单状态栏展示相应工单的处理节点进度，包括待下发、处理中、已完成、已撤回。

各工单状态及说明如下表所示：

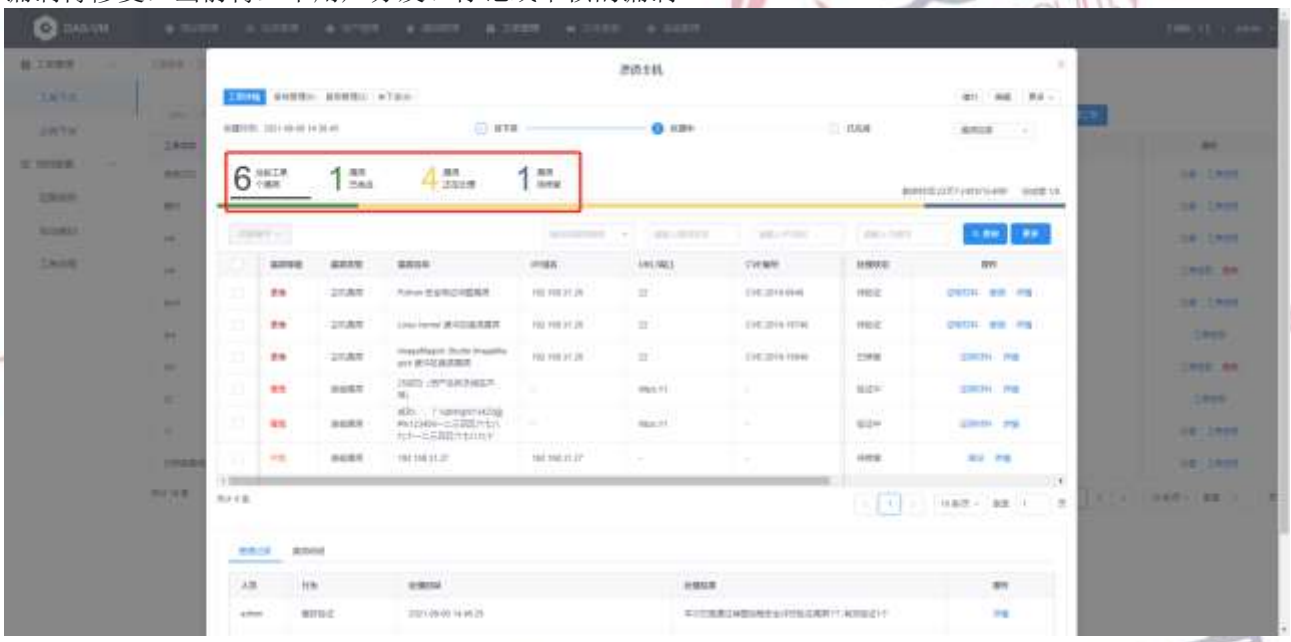
工单状态	说明
待下发	工单中没有漏洞下发至对应漏洞责任人。
处理中	工单中已有至少一个漏洞已进行通过工单平台下发至对应的漏洞责任人。
已完成	工单中除搁置漏洞和误报漏洞外所有漏洞经复扫后均验证为已修复。
已撤回	已撤回的工单，工单中的漏洞可重新创建工单并下发。

7.1.2.4. 工单编辑

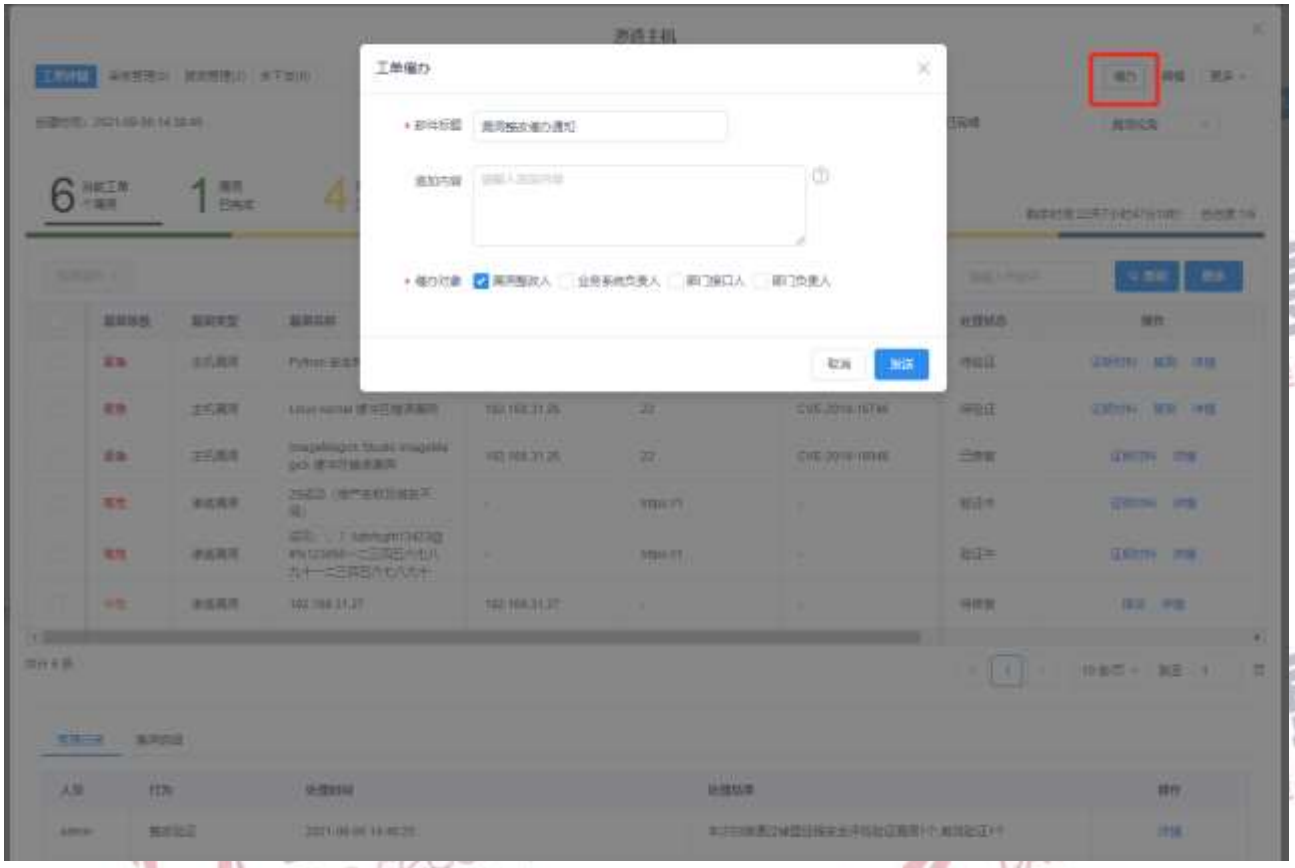
（1） 选择需撤回的工单，点击工单列表的<工单信息>按钮，展开工单信息。



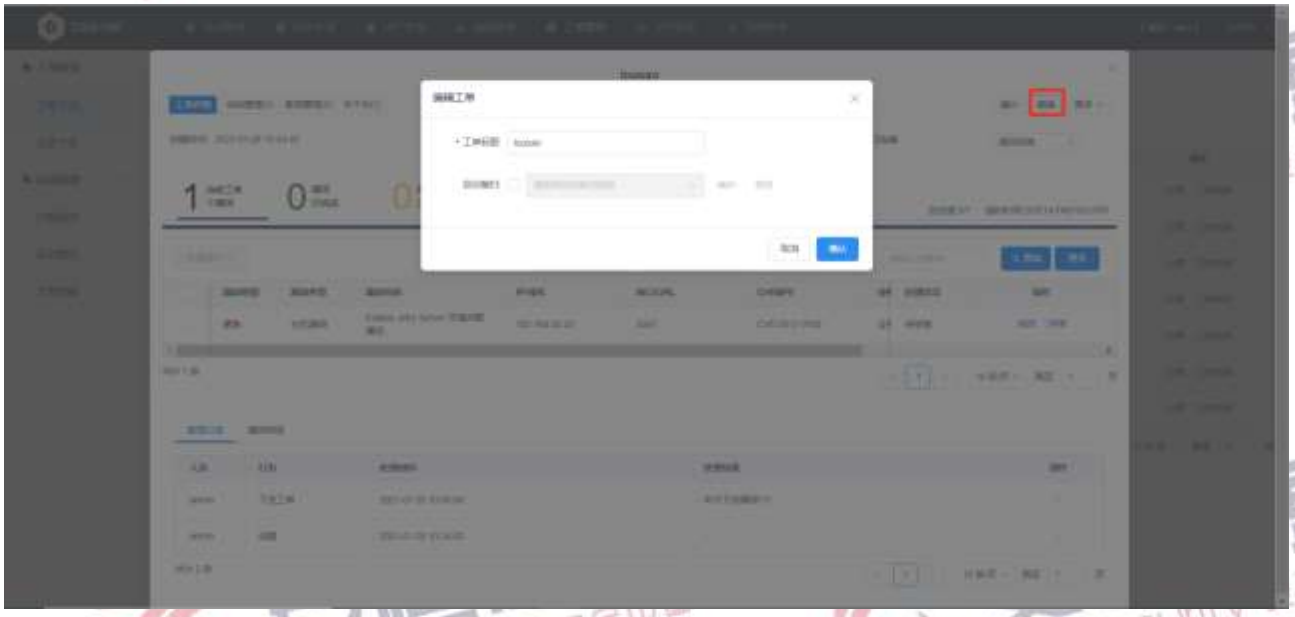
（2） 点击工单信息可以看到当前工单下相关漏洞处理信息：
当前工单漏洞：当前工单存在的所有漏洞；
漏洞已完成：当前审核通过或复测结果为已修复的漏洞；
漏洞正在处理：当前待审核或待复测的漏洞；
漏洞待修复：当前待工单用户分发、标记或审核的漏洞



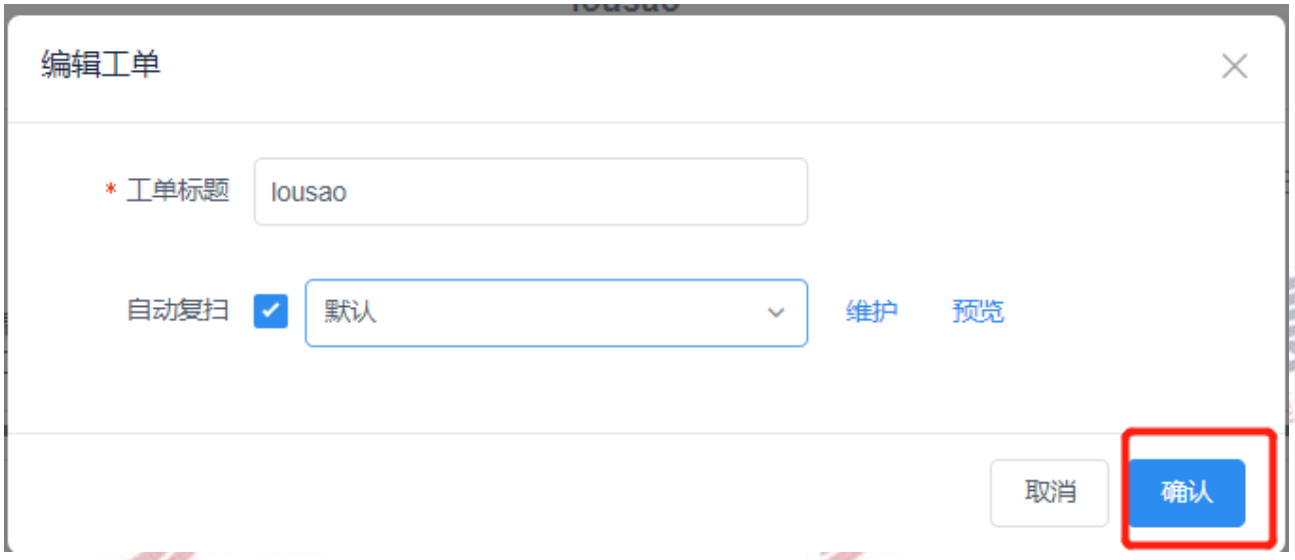
（3） 点击工单信息右上方的<催办>按钮，可以进行工单催办。可手动勾选漏洞资产所在业务系统负责人、漏洞责任人所在部门接口人、漏洞责任人所在部门负责人和当前漏洞处理人发送催办通知，催办对象可多选。催办通知支持邮件和短信形式。。



（4） 点击工单信息右上方的<编辑>按钮，可修改工单名称，重新选择是否开启自动复扫以及自动复扫规则，点击<维护>按钮可新增窗口并进入[工单管理/规则配置/自动复扫]页面进行自动复扫规则编辑，点击<预览>按钮可查看所选自动复扫规则的详细内容。

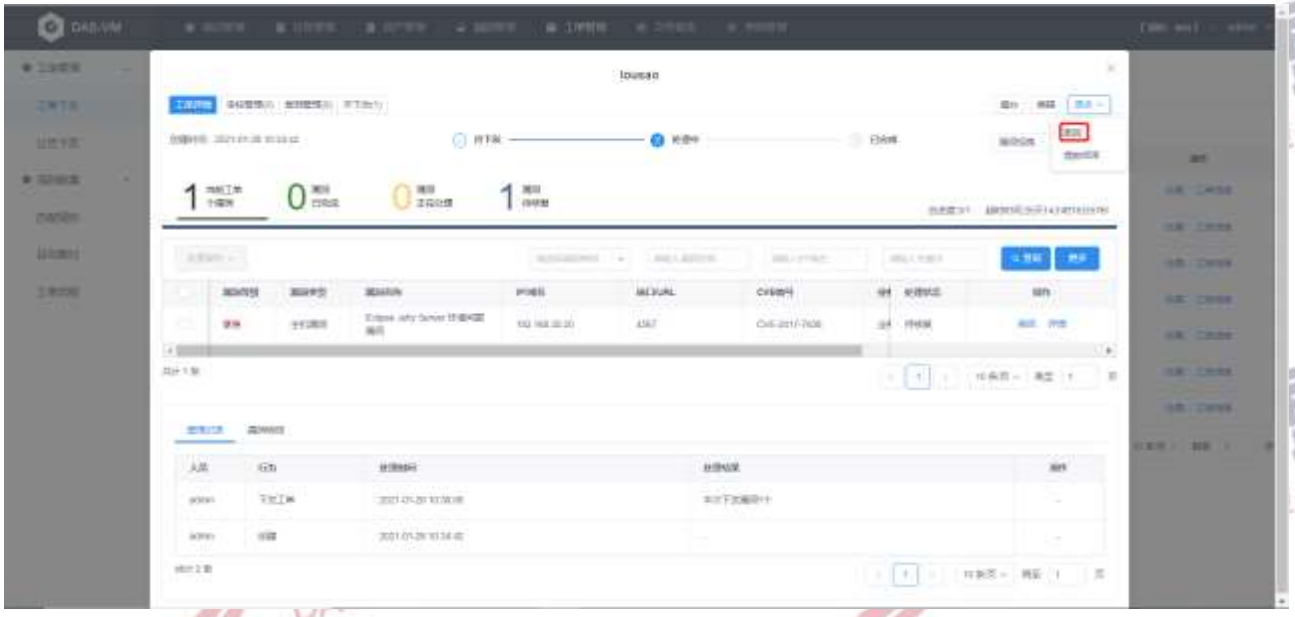


（5） 编辑完成后点击<确认>按钮即可完成编辑，自动复扫规则将在下一次触发规则时生效。

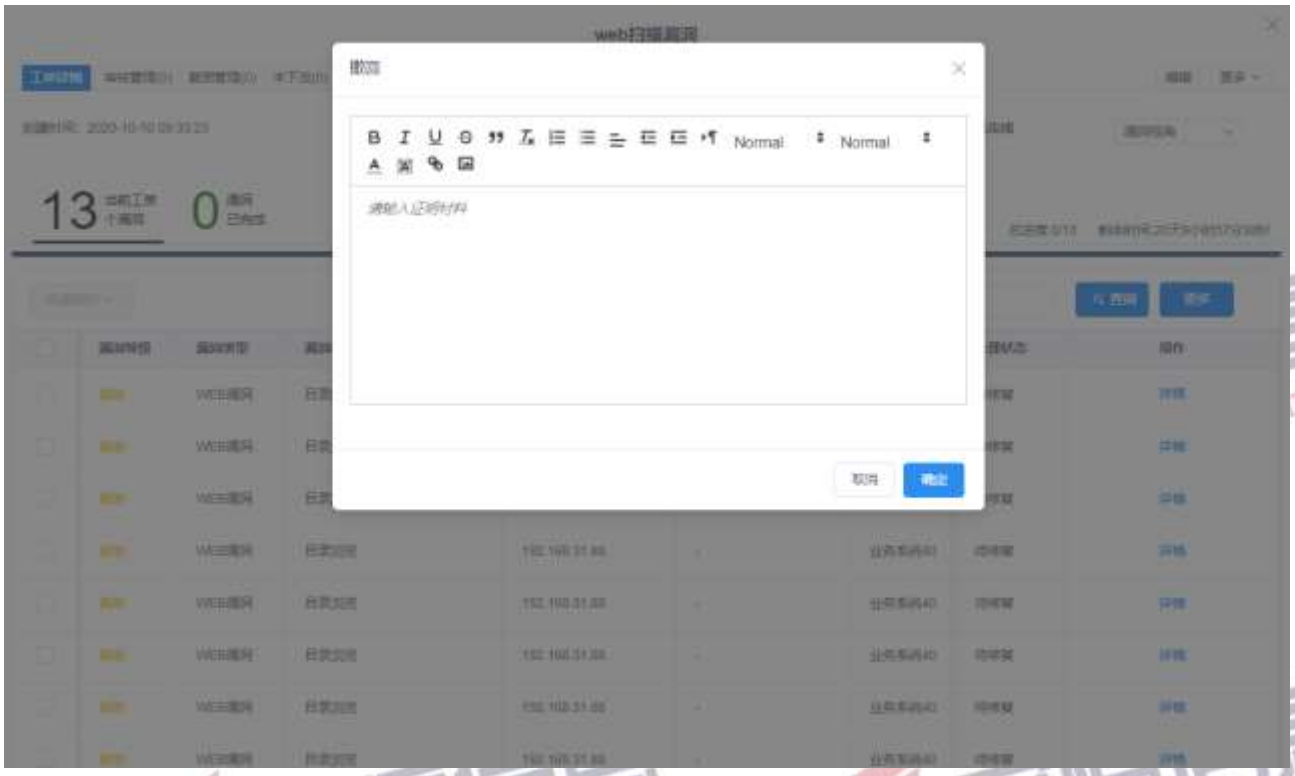


7.1.2.5. 工单撤回

（1） 点击工单信息右上方的<更多>按钮，下拉展示<撤回>按钮。撤回工单时，可向当前待处理漏洞的处理人发送撤回通知，撤回通知支持邮件和短信两种形式。

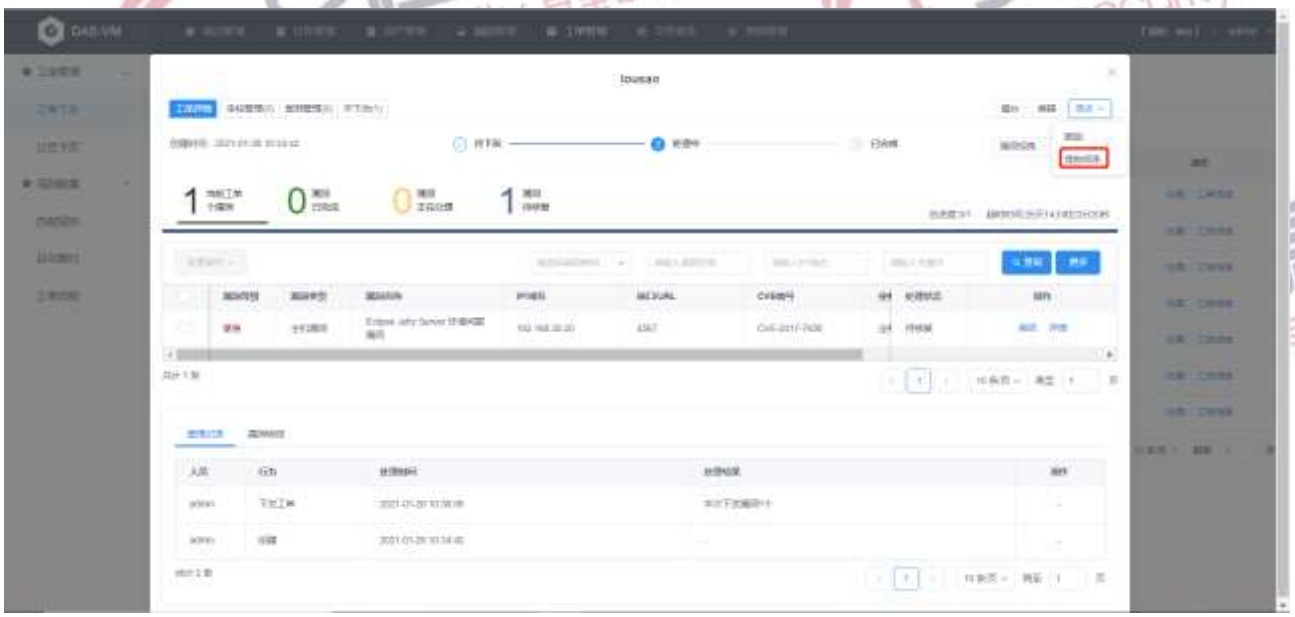


（2） 点击<撤回>按钮，填写撤回原因及证明，点击<确定>按钮，可撤回该工单，工单中的漏洞可重新创建工单并下发。

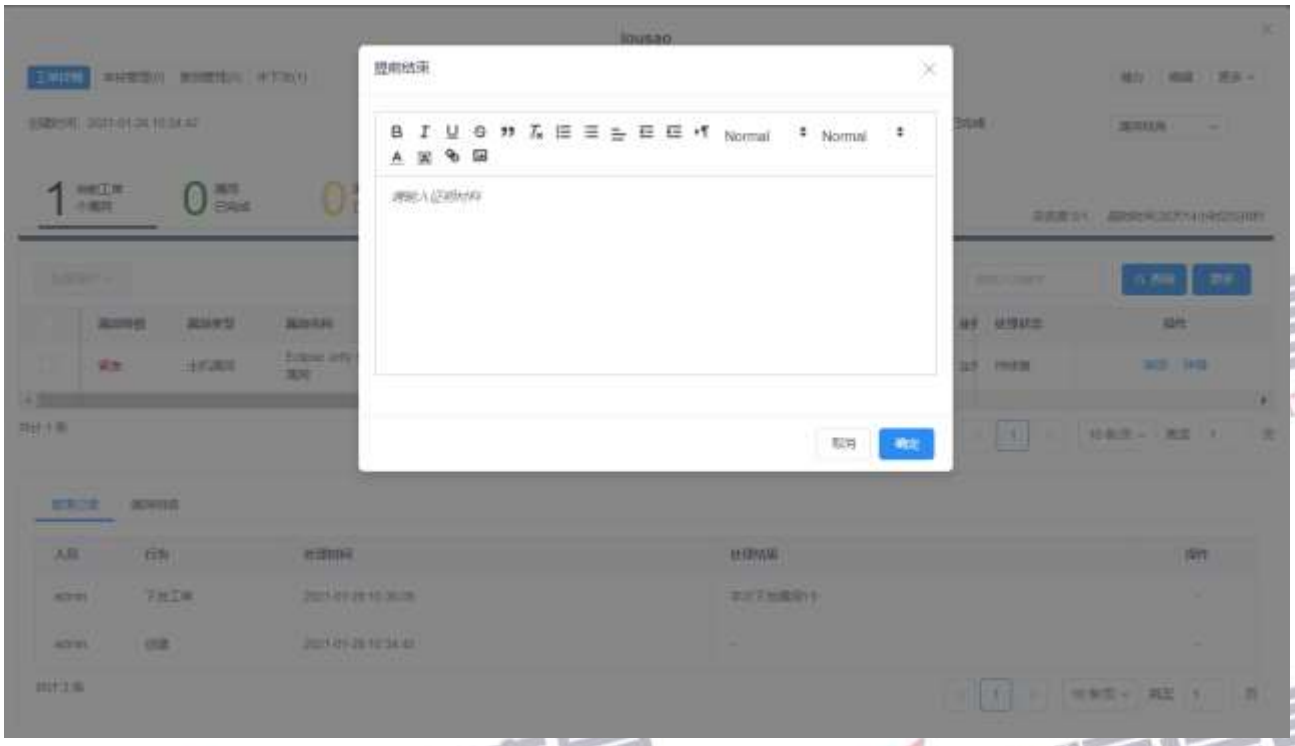


7.1.2.6. 工单提前结束

（1） 点击工单信息右上方的<更多>按钮，下拉展示<提前结束>按钮。

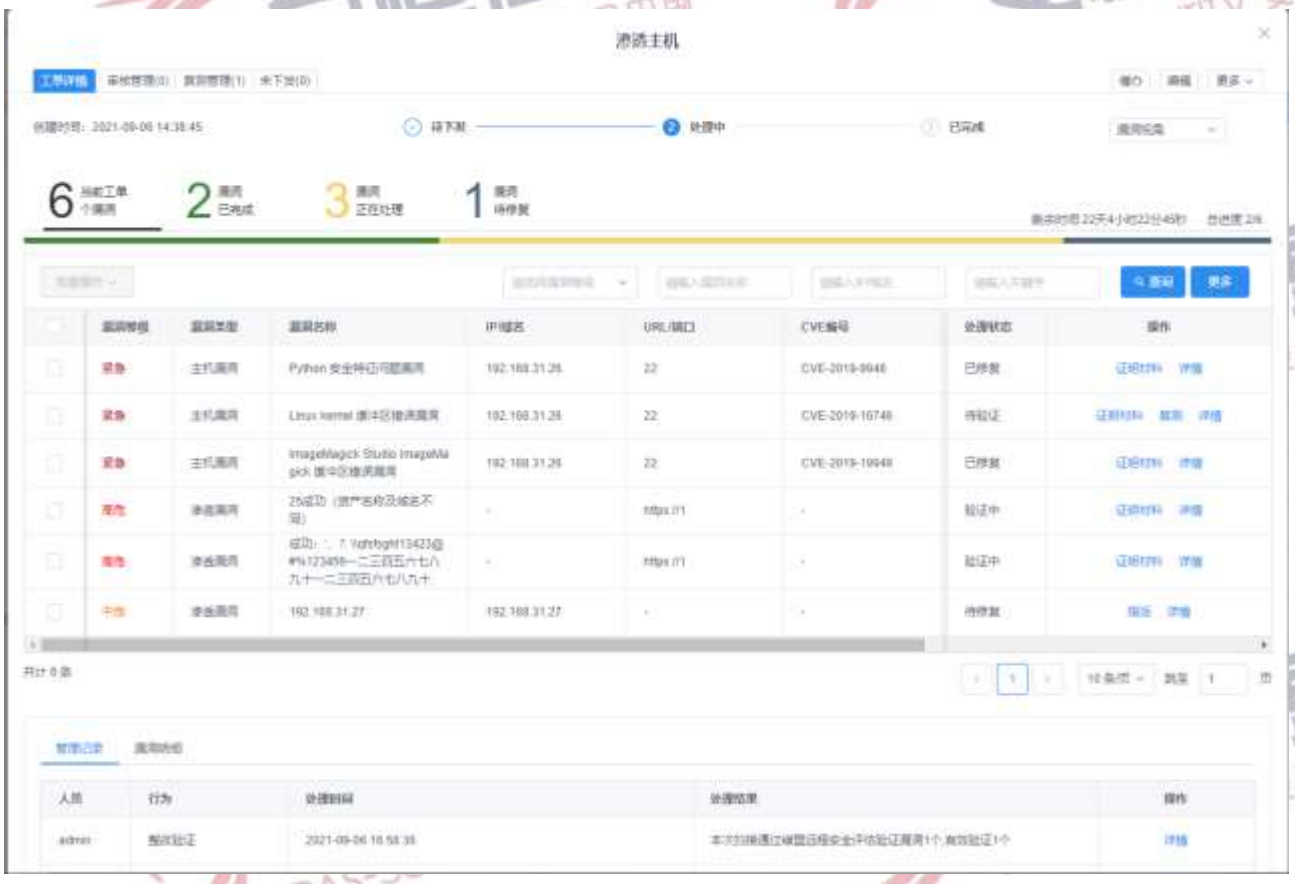


（2） 点击<提前结束>按钮，填写提前结束原因及证明，点击<确定>按钮，可提前结束该工单。增加提前结束工单功能，管理员可提前结束工单，保留当前已审核和已复测的漏洞，其他漏洞可通过重新创建工单并下发。提前结束工单时，可向当前待处理漏洞的处理人发送提前结束通知。提前结束通知支持邮件和短信两种形式。



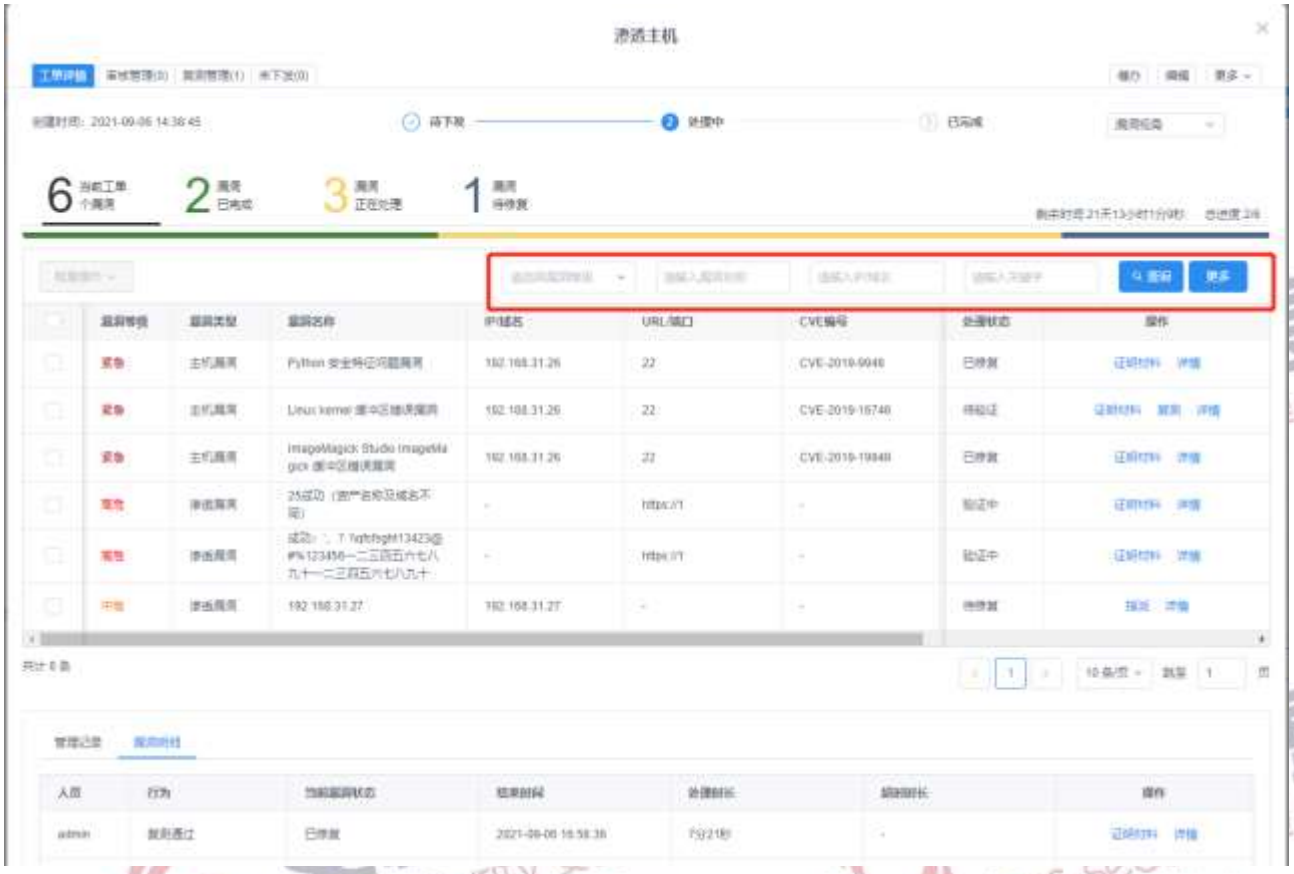
7.1.2.7. 工单详情

（1） 选择工单，点击工单列表的<工单信息>按钮，展开工单信息，默认展示工单详情的漏洞视角。

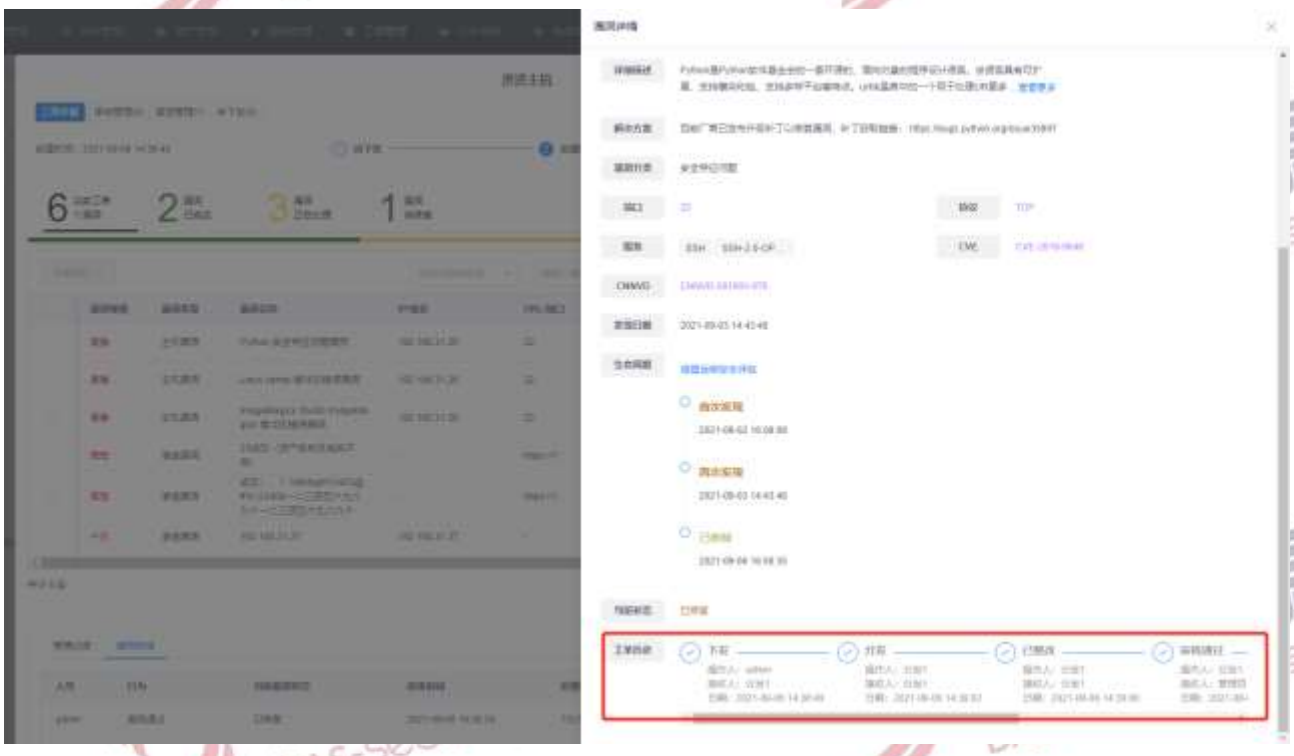


（2） 点击右上方漏洞视角下拉展开更多视角选项，点击可切换不同视角下该工单的统计信息。业务系统视角、漏洞责任人视角、资产责任人视角和工单节点视角的漏洞以不同的视角展示，点击列表中<查看>，可以跳转到相应的漏洞界面。

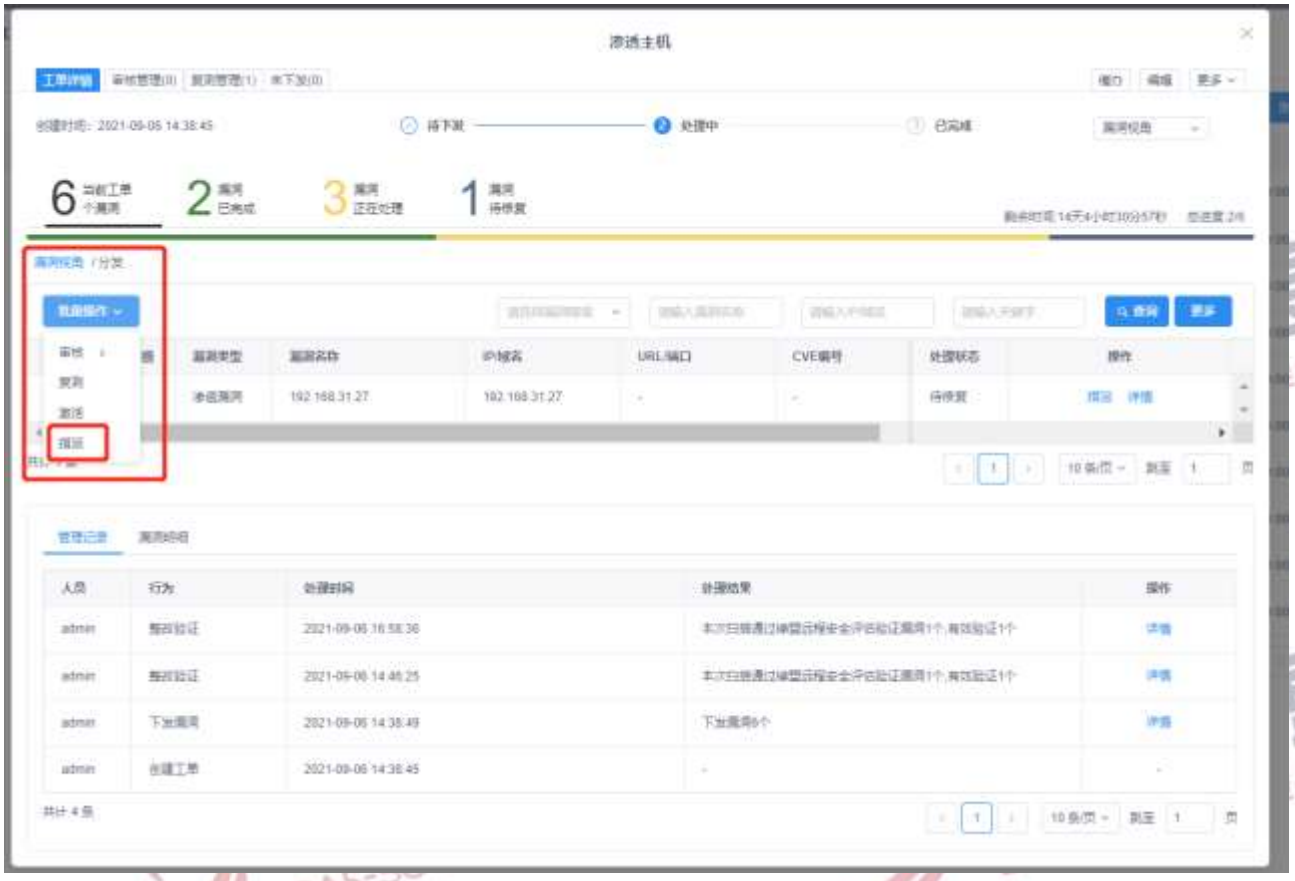
（3） 设置查询条件，可在漏洞列表中进行指定漏洞查询。设置条件后，点击<查询>按钮，进行查询。也可点击<更多>按钮，下拉展开更多的查询条件，设置条件后，点击<查询>按钮，进行查询。



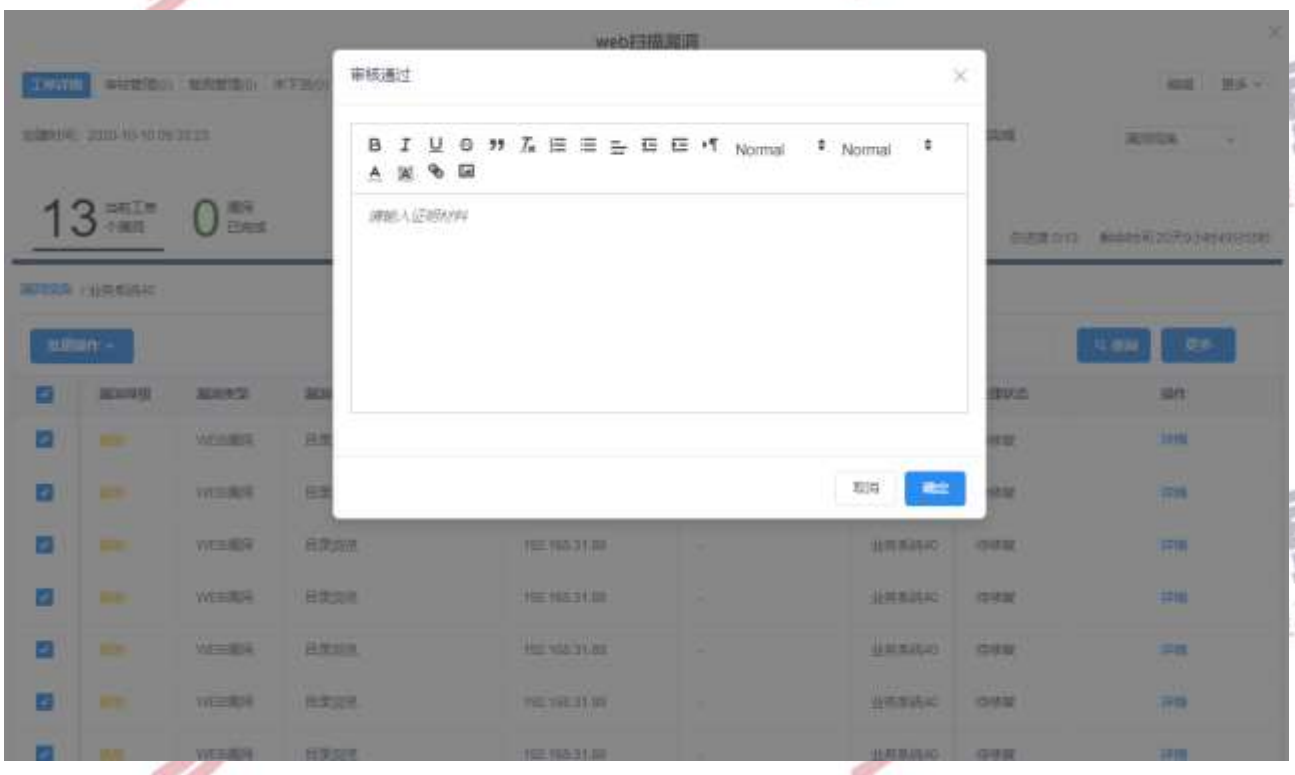
（4）点击漏洞列表<详情>按钮可查看漏洞的详细信息，并且可以快速查看到该漏洞的工单历史信息，洞悉该漏洞的流转。



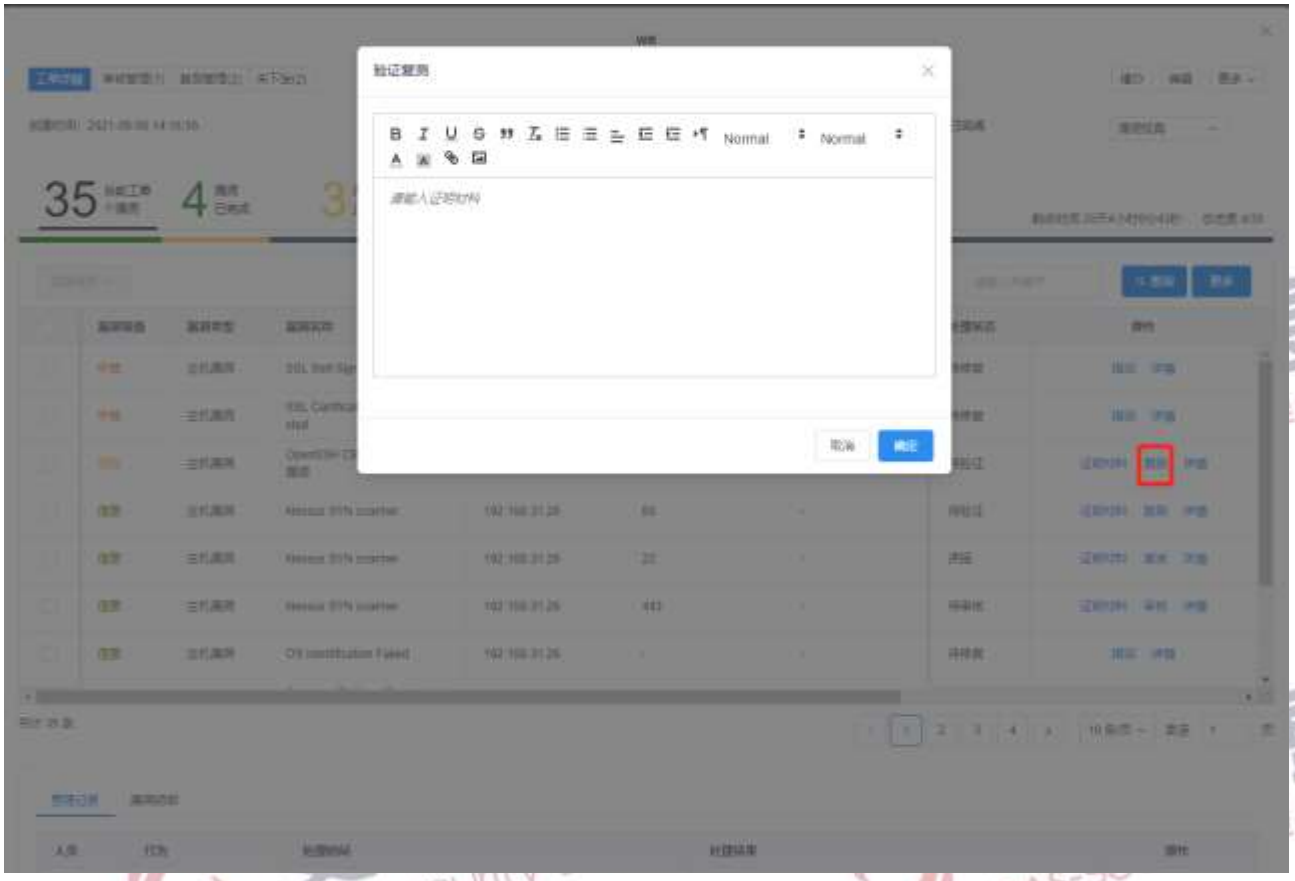
（5）勾选漏洞点击<批量操作>按钮下拉展示操作选项可快速进行漏洞处理，其中工单节点视角的漏洞可以进行指派的批量操作。



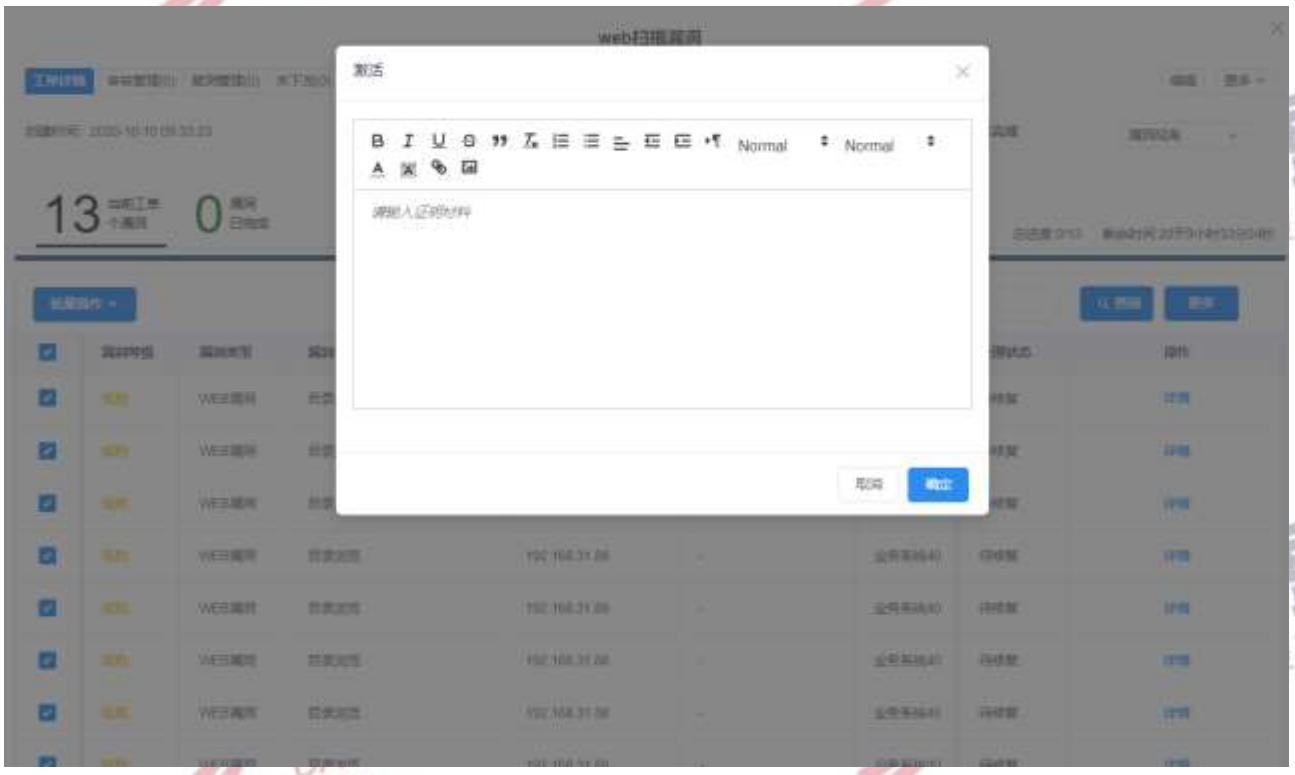
（6） 点击<审核>按钮，选择审核通过或审核不通过，填写证明材料，点击<确定>按钮即可完成待审核漏洞的审核。



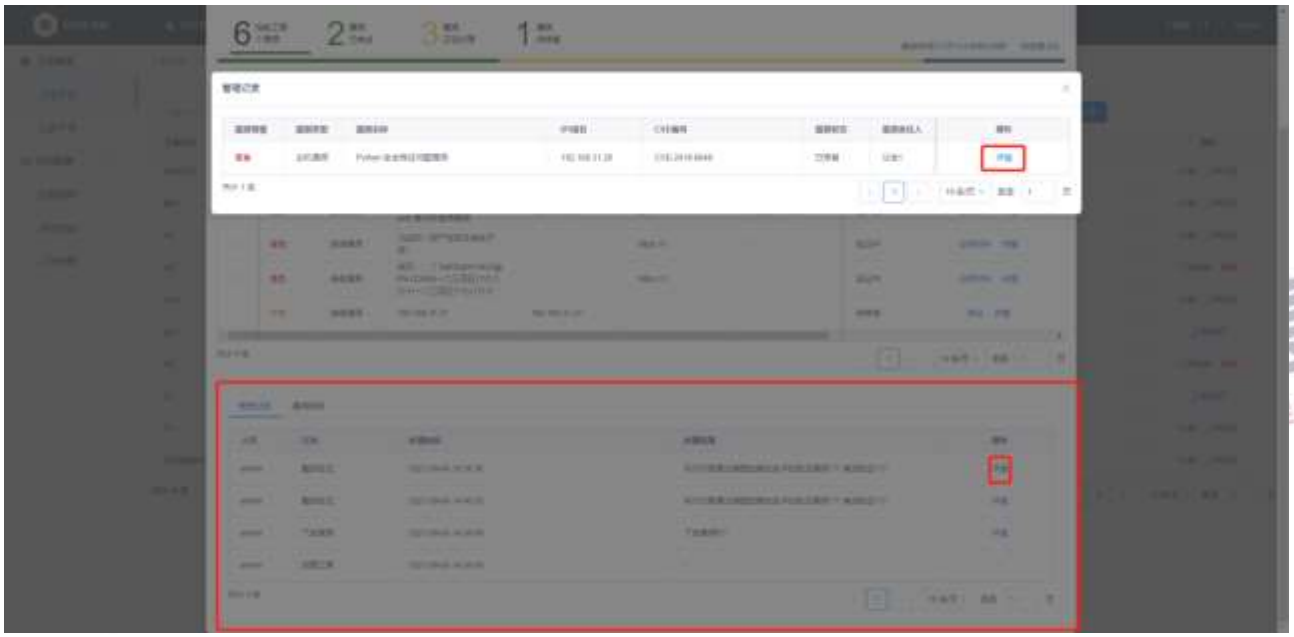
（7） 点击<复测>按钮，填写证明材料，点击<确定>按钮即可对待复测的漏洞发起复测。



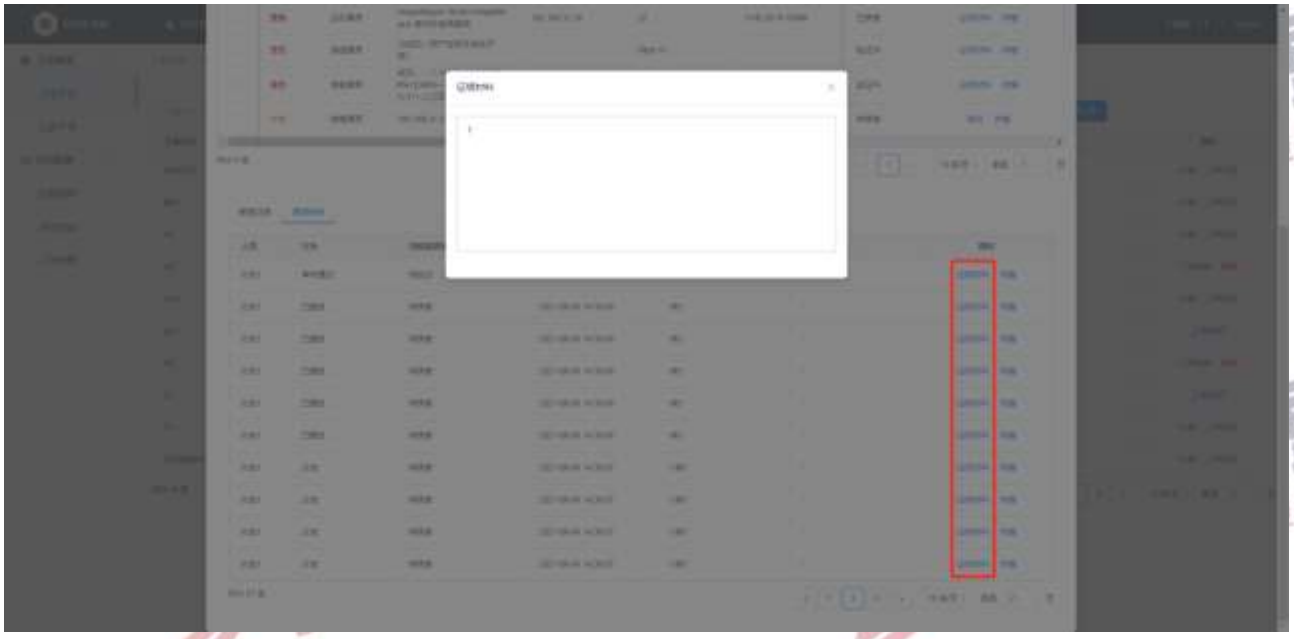
（8） 点击<激活>按钮，填写证明材料，点击<确定>按钮即可激活搁置漏洞或误报漏洞并下发至工单系统对应漏洞责任人手上。



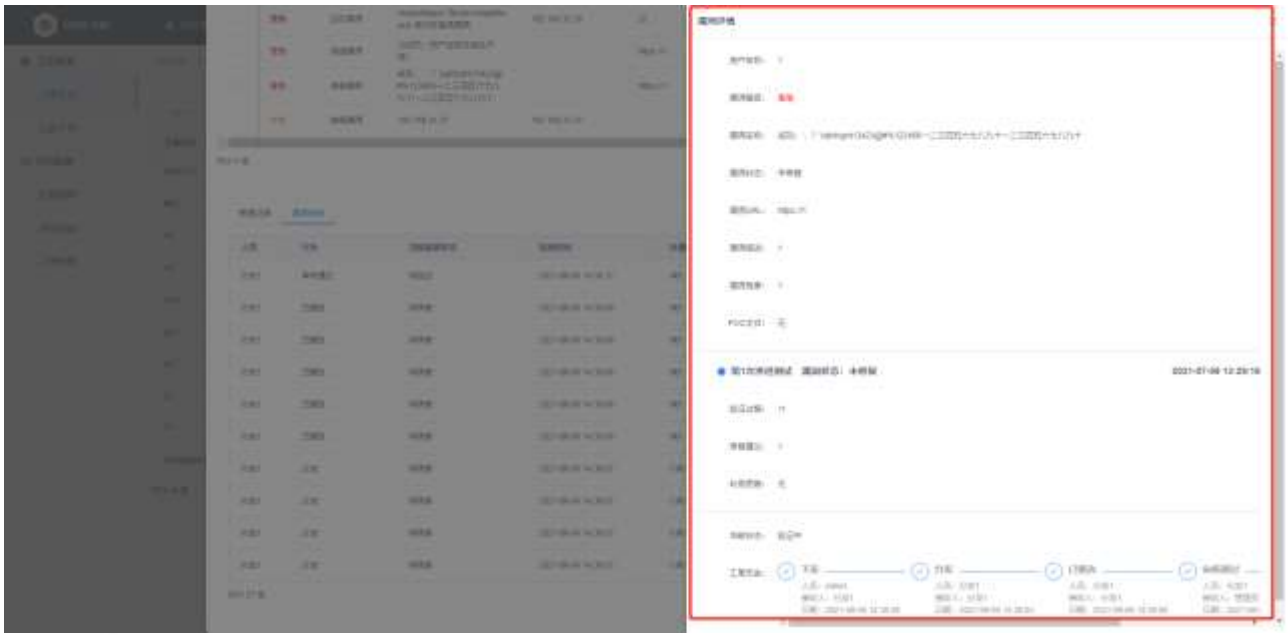
（9） 工单详情可以查看管理记录和漏洞明细。点击管理记录中的<详情>，查看详细的管理记录，然后点击相关漏洞的<详情>按钮，查看改漏洞的详细信息。



（10） 点击漏洞明细中的<详情>，查看详相关漏洞的操作证明材料以及详细信息。

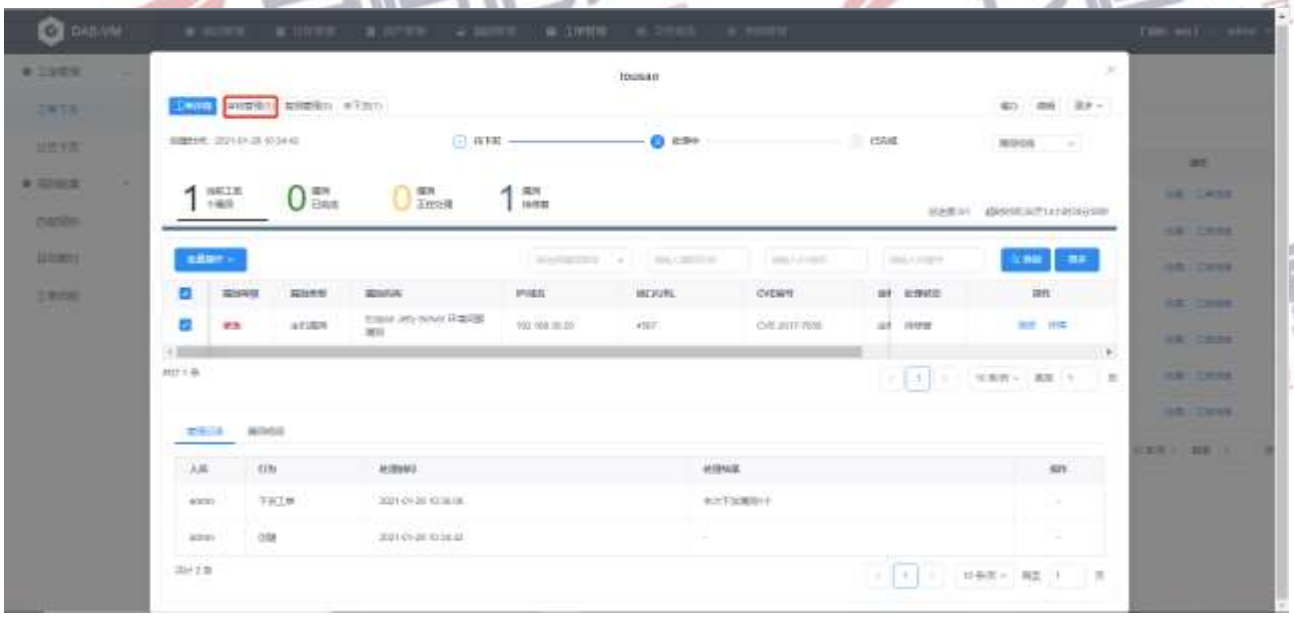


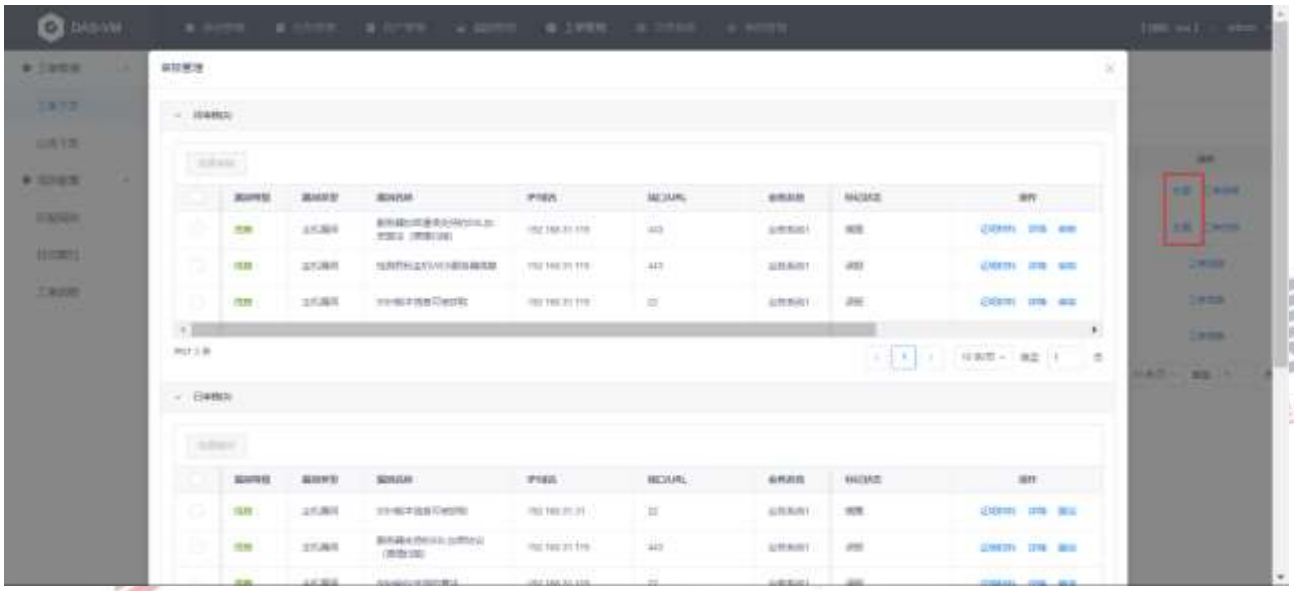
（11） 点击漏洞明细中的<详情>按钮，查看改漏洞的详细信息，点击<证明材料>按钮查看相关材料。



7.1.2.8. 审核管理

（1） 选择工单，点击工单列表的<工单信息>按钮，展开工单信息，点击<审核管理>进入审核管理页面。也可点击工单列表的<处置>按钮快速进入审核管理页面





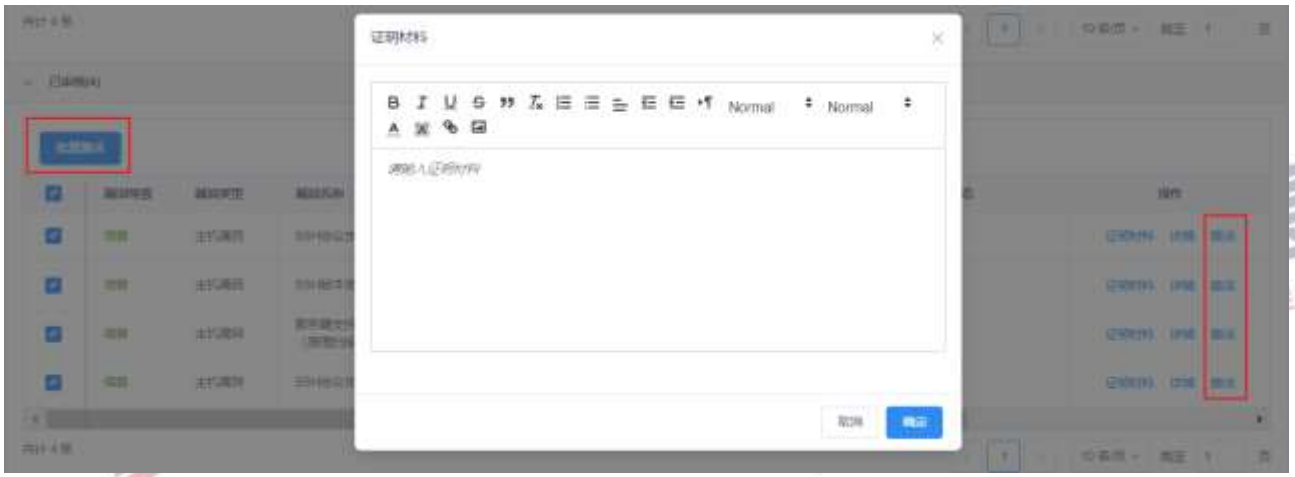
（2） 点击待审核漏洞列表或已审核漏洞列表的<详情>按钮可查看对应漏洞的详细信息。

（3） 点击待审核漏洞列表的<证明材料>按钮可查看对应漏洞标记为搁置或误报时的证明材料。

（4） 待审核漏洞列表选择漏洞点击<审核>按钮或勾选漏洞点击<批量审核>按钮，选择审核通过或审核不通过，填写证明材料，点击<确定>按钮即可完成待审核漏洞的审核。审核通过的漏洞，从待审核列表移入已审核列表；审核不通过的漏洞将重新下发至工单系统第一个节点的漏洞责任人。

（5） 点击已审核漏洞列表的<证明材料>按钮可查看对应漏洞审核通过时的证明材料。

（6） 若需要激活已审核的搁置漏洞或误报漏洞，可在已审核漏洞列表选择漏洞点击<激活>按钮或勾选漏洞点击<批量激活>按钮，填写证明材料，点击<确定>按钮即可完成已审核漏洞的激活。激活的漏洞将重新下发至工单系统第一个节点的漏洞责任人。

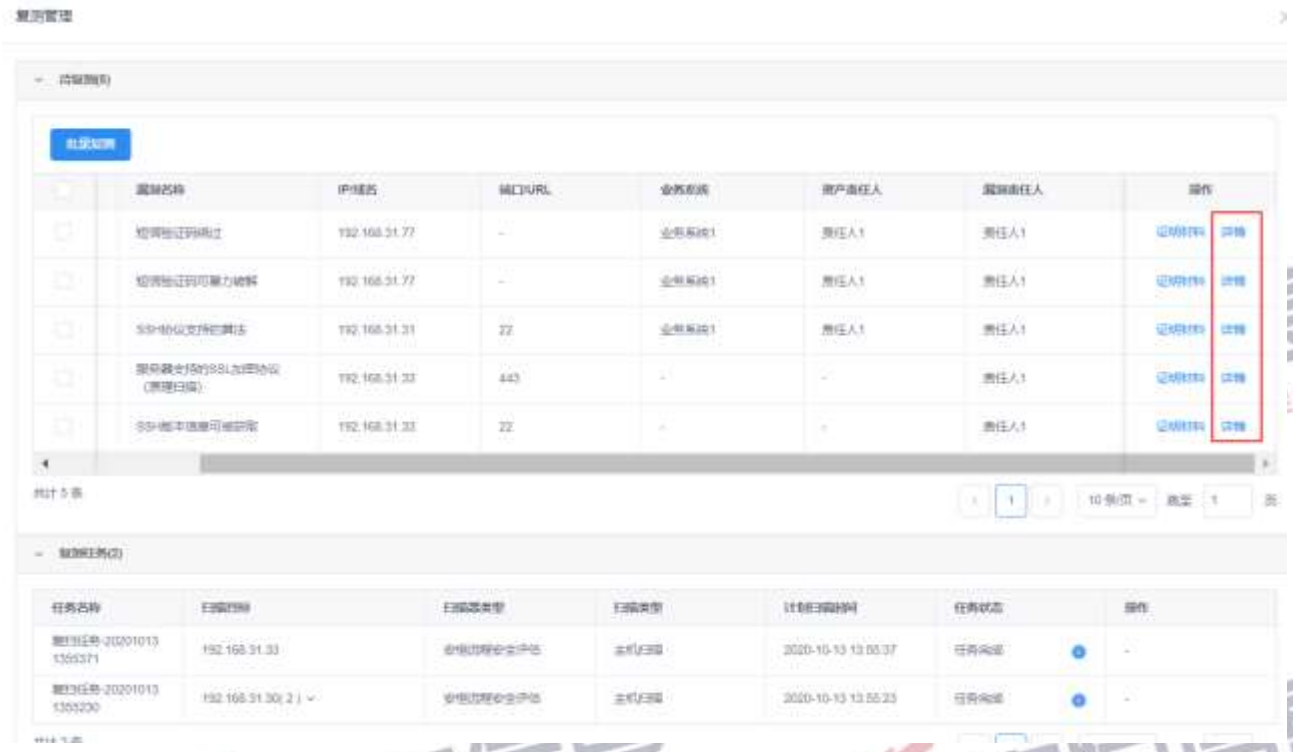


（7） 历史信息记录了审核通过和审核不通过的操作记录，点击<证明材料>按钮可查看对应漏洞审核通过或不通过时的证明材料。

7.1.2.9. 复测管理

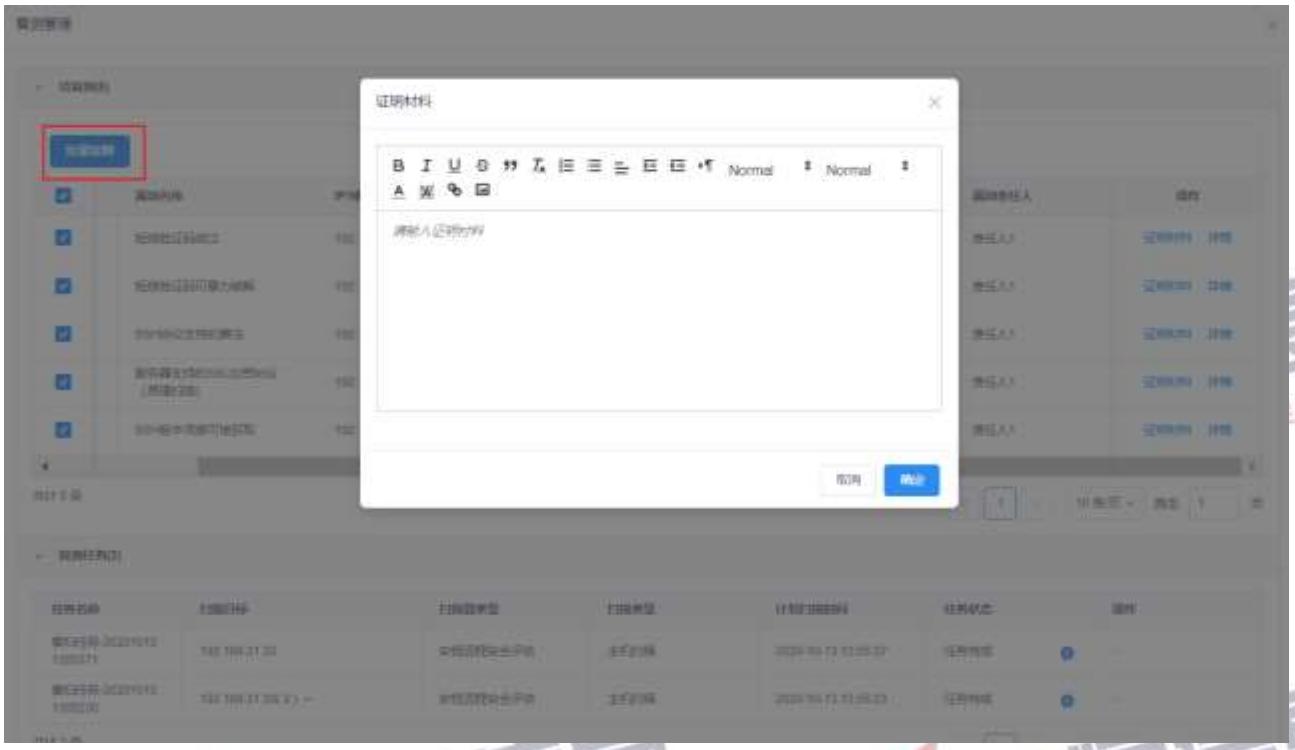
（1） 选择工单，点击工单列表的<工单信息>按钮，展开工单信息，点击<复测管理>进入复测管理页面。

（2） 点击待复测漏洞列表的<详情>按钮可查看对应漏洞的详细信息。



（3） 点击待复测漏洞列表的<证明材料>按钮可查看对应漏洞标记为已整改时的证明材料。

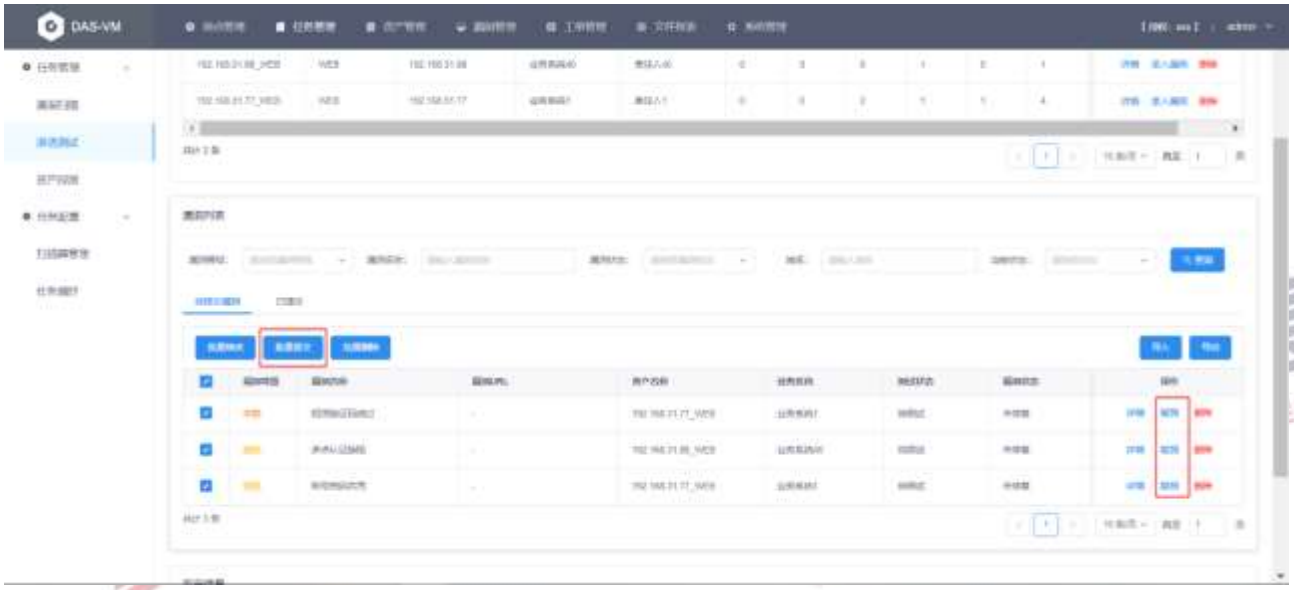
（4） 待复测漏洞列表勾选漏洞点击<批量复测>按钮，填写证明材料，点击<确定>按钮即可发起待复测漏洞的复测。若该工单开启自动复扫将在允许扫描时段统计待复测漏洞，符合自动复扫规则的漏洞将自动发起复测。



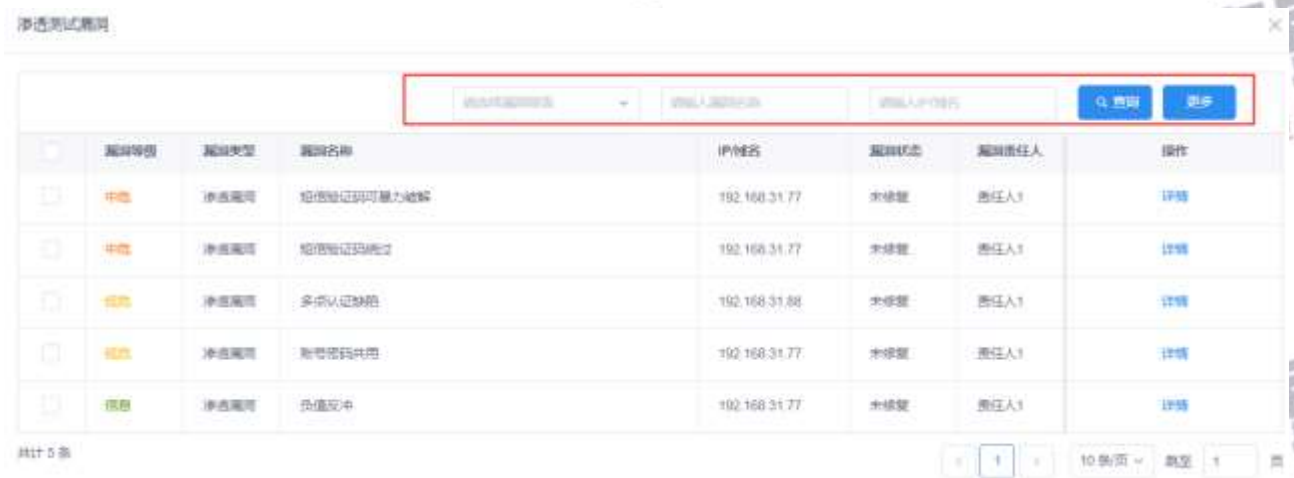
（5） 扫描发现的漏洞将调用最新一次的扫描任务参数发起复扫，执行中任务可点击<停止>按钮或<暂停>按钮停止或暂停任务；扫描报告导入的漏洞需要重新导入一次扫描报告；

（6） 渗透录入的漏洞需进入渗透测试任务详情的待提交漏洞列表进行复测，可点击渗透任务列表的<详情>按钮快速进入对应渗透测试任务详情页的待提交漏洞列表进行漏洞复测。

（7） 渗透测试任务详情页的待提交漏洞列表点击<复测>按钮，输入漏洞测试信息，包括漏洞状态、验证过程、修复建议和利用思路。然后勾选已复测漏洞点击<批量提交>按钮完成漏洞的复测。



（8） 点击渗透任务列表的<漏洞列表>按钮可查看该工单下该渗透任务的所有漏洞。可设置查询条件，点击<查询>按钮进行指定漏洞查询；也可点击<更多>按钮，下拉展开更多的查询条件，设置条件后，点击<查询>按钮进行查询。点击漏洞列表的<详情>按钮可查看对应漏洞的详细信息。



（9） 复扫任务扫描完成或渗透侧试复测漏洞提交完成可在历史信息列表查看复测结果，点击<详情>按钮可查看具体该次扫描或提交的漏洞的复测详情。复测结果为已修复的漏洞将结束工单流程，复测结果为未修复的漏洞将重新下发至工单系统第一个节点的漏洞责任人。

7.2. 规则配置

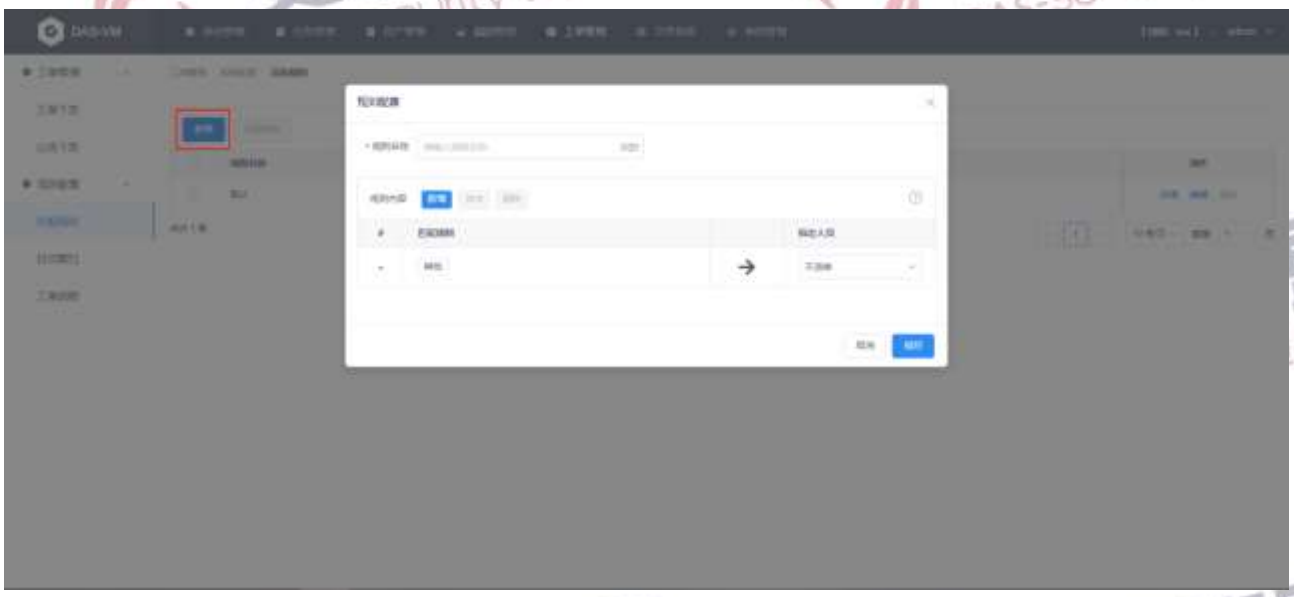
7.2.1. 匹配规则

用于创建工单时将所有漏洞按指定规则匹配相应工单系统的漏洞责任人。

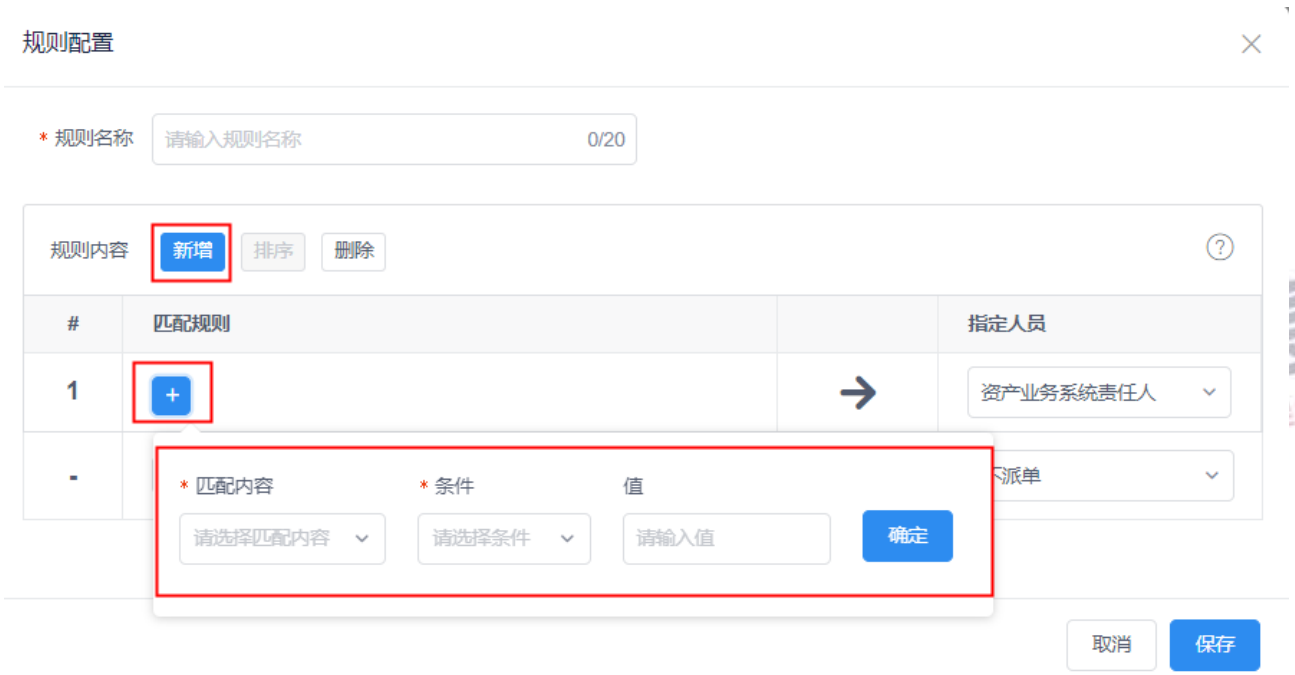
7.2.1.1. 新增匹配规则

（1） 用户 WEB 登录后，进入[工单管理 /规则配置/匹配规则]页面。

（2） 点击<新增>按钮，在新增规则配置窗口，填写规则名称。规则名称长度不超过 20 个字符。



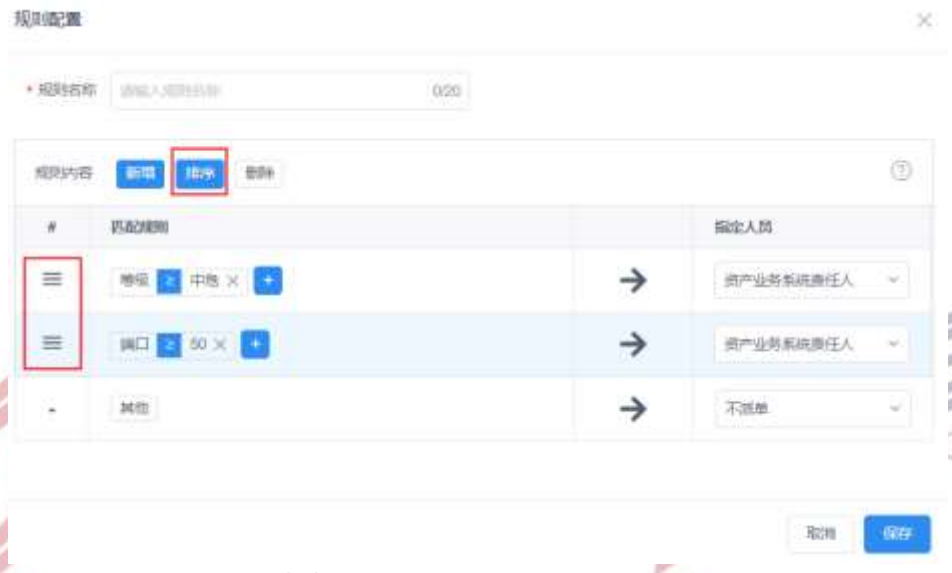
（3） 新增规则配置窗口点击<新增>按钮新增规则行，点击 + 符号下拉选择匹配内容、条件并输入值，点击<确定>按钮，选择指定人员类型即可完成单条规则创建。指定人员类型包括资产业务系统责任人、资产责任人、端口业务系统责任人、端口责任人、指定人员、不派单六种，选择指定人员时需选择具体人员。



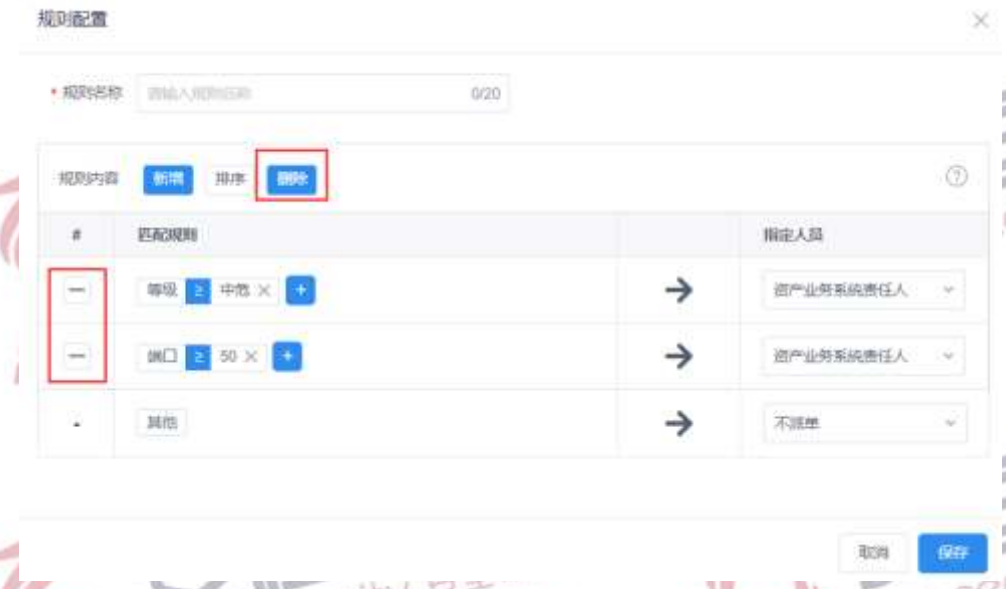
匹配规则各匹配内容对应条件和值说明如下：

匹配内容	条件	值
等级	可选＝、≥、≤	下拉选择：信息、低危、中危、高危、紧急
漏洞名称	可选包含、＝	输入文本
端口	可选＝、≥、≤	输入范围为 1-65535 的整数，
漏洞类型	可选＝	下拉选择：主机漏洞、WEB 漏洞、基线漏洞、弱口令漏洞、数据库漏洞、渗透漏洞
服务	可选包含、＝	输入文本
CVE 编号	可选包含、＝	输入文本

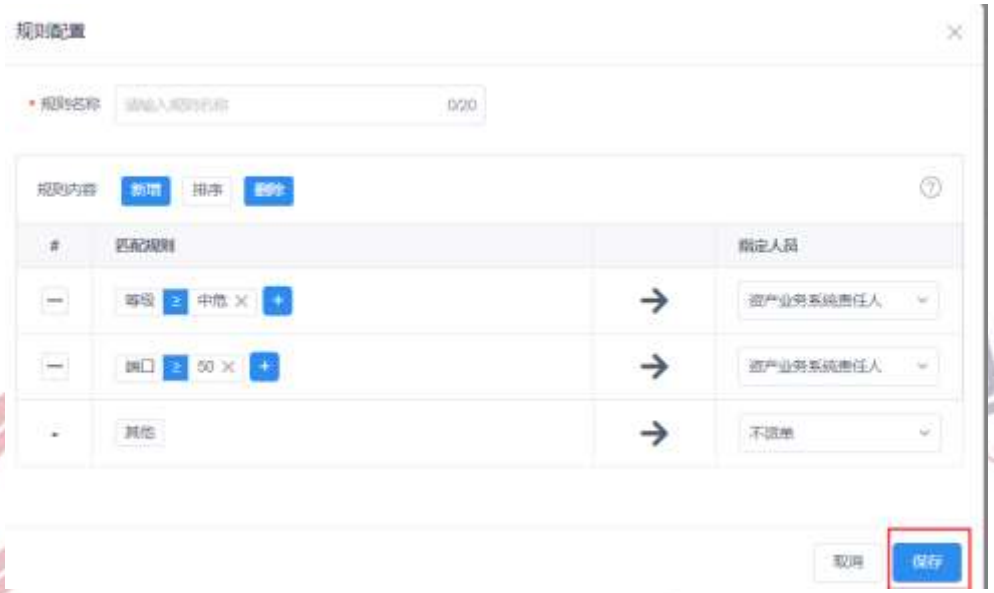
（4）新增多行规则行，点击<排序>按钮，上下拖动列表前 ☰ 符号可改变规则行上下顺序。



（5） 点击<删除>按钮，点击列表前 — 符号可删除规则行。



（6） 规则条件设定完成后，点击<保存>按钮，即可新增新的匹配规则。



7.2.1.2. 编辑匹配规则

（1） 点击匹配规则列表的<详情>按钮，可查看匹配规则详细内容。

（2） 点击匹配规则列表的<编辑>按钮，在编辑规则配置窗口，修改规则名称和规则条件。点击<新增>按钮新增规则行，点击 + 符号下拉选择匹配内容、条件并输入值，点击<确定>按钮，选择指定人员类型即可完成单条规则创建；点击<删除>按钮，点击列表前 − 符号可删除规则行；点击<排序>按钮，上下拖动列表前 ≡ 符号可改变规则行上下顺序；点击<保存>按钮即可完成匹配规则的编辑。

7.2.1.3. 默认匹配规则

（1） 点击匹配规则列表规则名称后的<设为默认>按钮，即可将该规则设置为默认匹配规则，工单创建时默认优先选择默认匹配规则。

7.2.1.4. 删除匹配规则

（1） 点击匹配规则列表的<删除>按钮并确认，即可删除相应匹配规则；默认匹配规则无法删除。

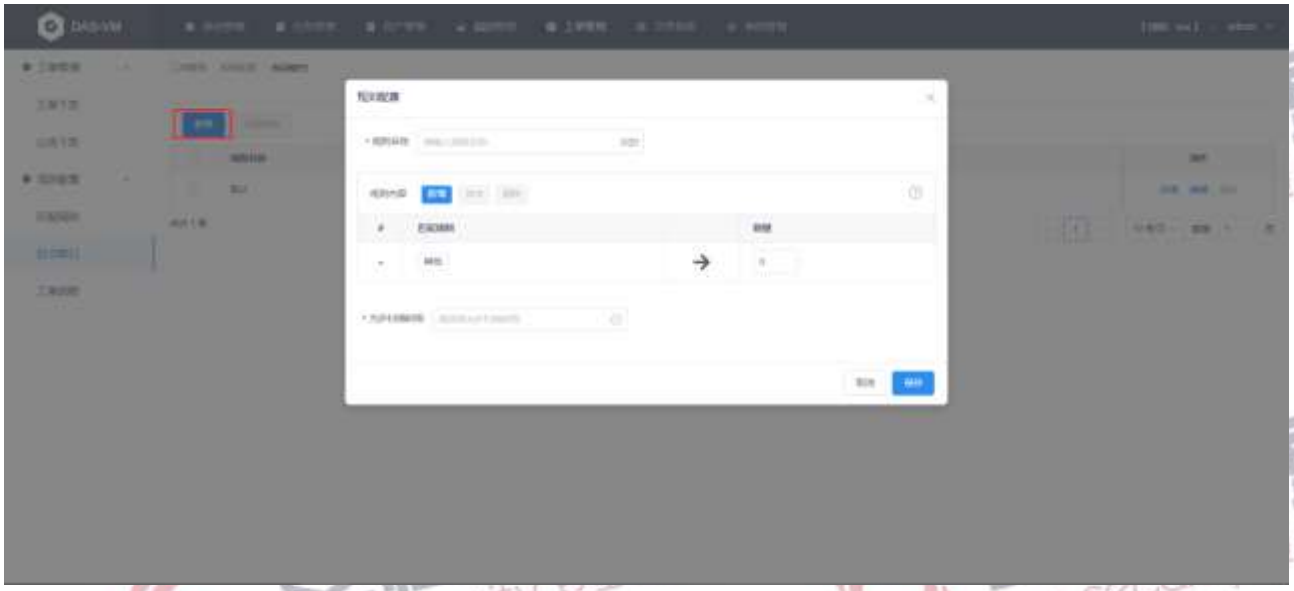
7.2.2. 自动复扫规则

用于工单复测时将所有待复测漏洞按指定自动复扫规则在允许扫描时段发起自动复测。

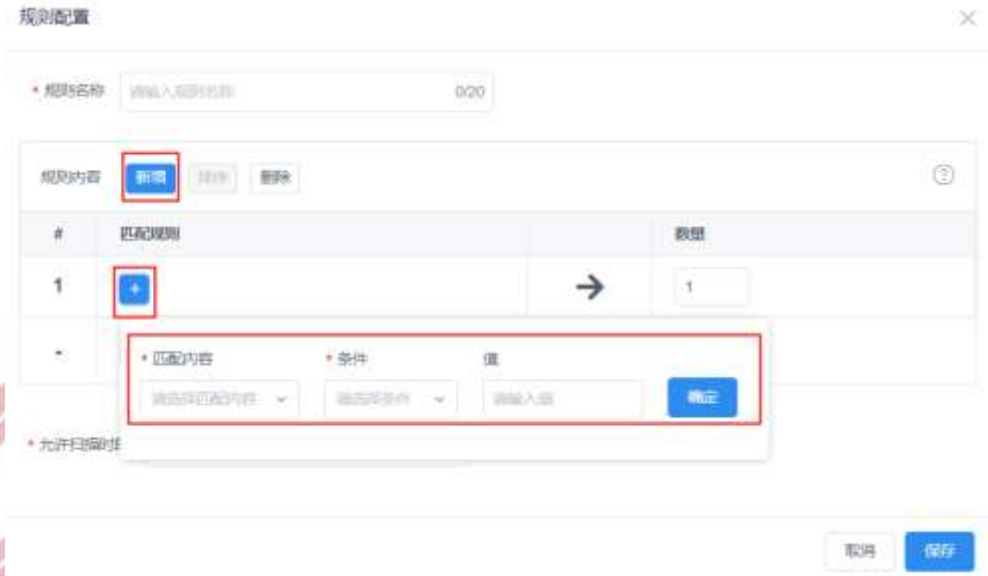
7.2.2.1. 新增自动复扫规则

（1） 用户 WEB 登录后，进入[工单管理 /规则配置/自动复扫]页面。

（2）点击<新增>按钮，在新增规则配置窗口，填写规则名称。规则名称长度不超过 20 个字符。



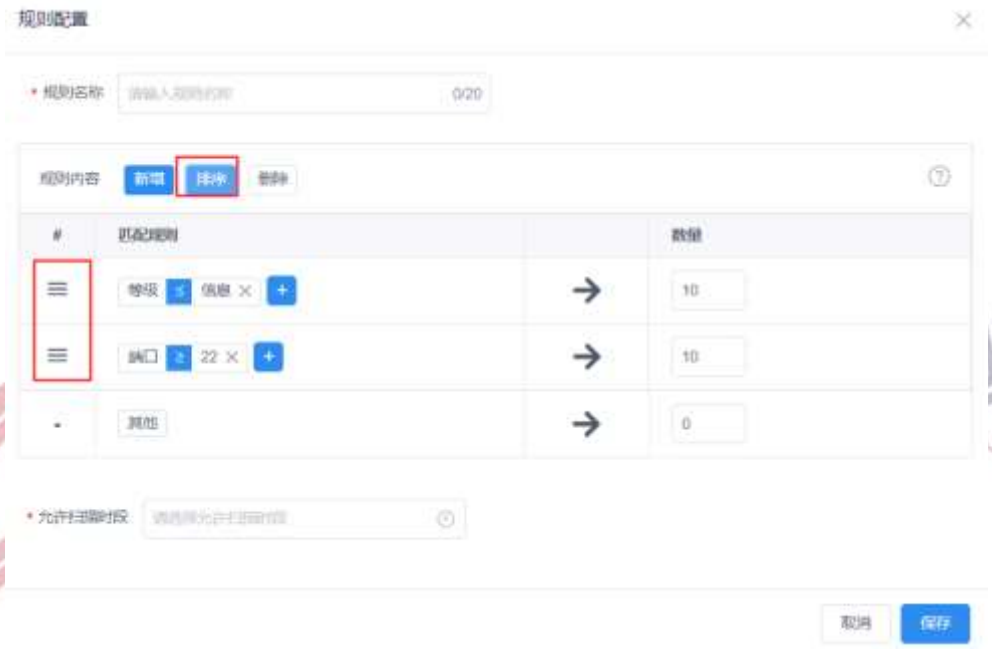
（3）新增规则配置窗口点击<新增>按钮新增规则行，点击 符号下拉选择匹配内容、条件并输入值，点击<确定>按钮，填写漏洞数量即可完成该条规则创建。



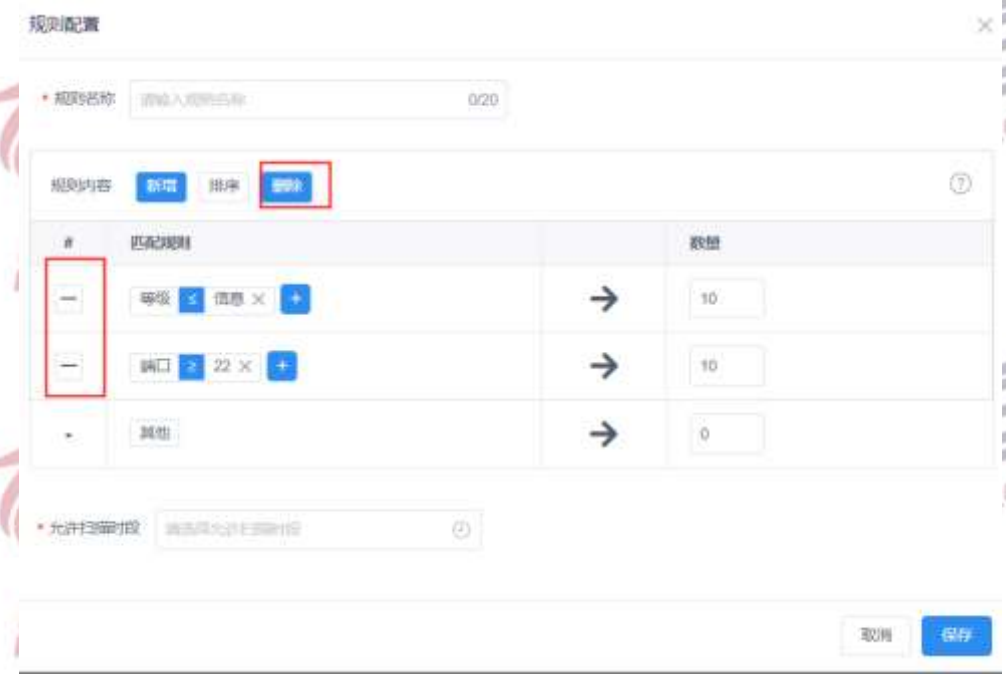
匹配规则各匹配内容对应条件和值说明如下：

匹配内容	条件	值
等级	可选＝、≥、≤	下拉选择：信息、低危、中危、高危、紧急
漏洞名称	可选包含、＝	输入文本
端口	可选＝、≥、≤	输入范围为 1-65535 的整数，
漏洞类型	可选＝	下拉选择：主机漏洞、WEB 漏洞、基线漏洞、弱口令漏洞、数据库漏洞、渗透漏洞
服务	可选包含、＝	输入文本
CVE 编号	可选包含、＝	输入文本

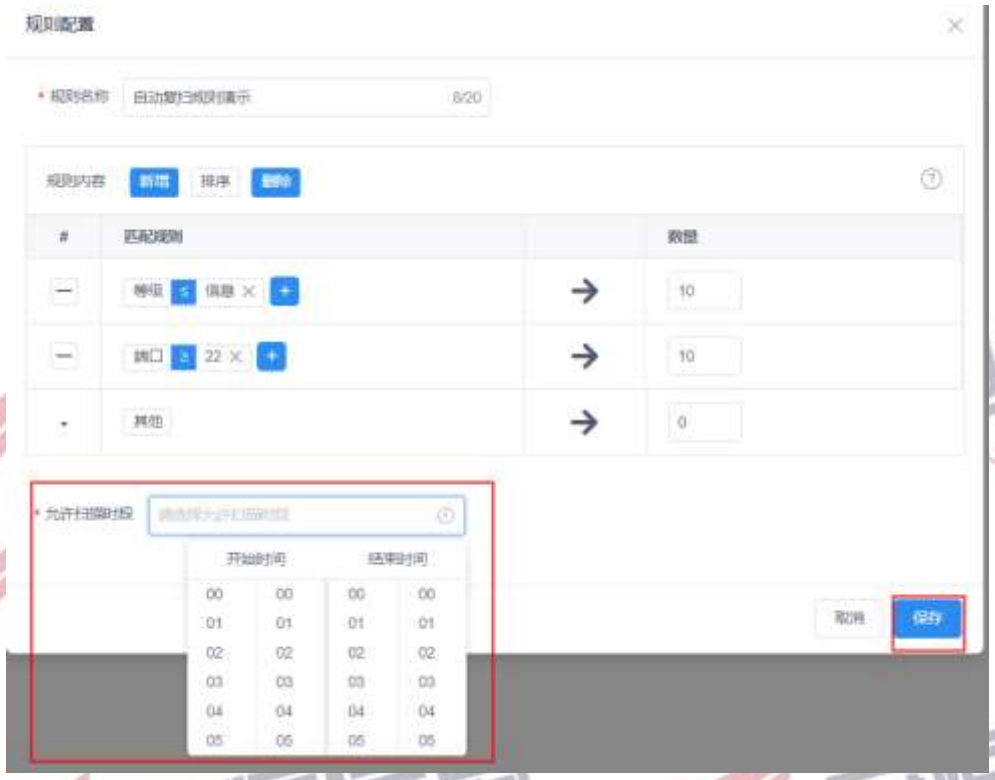
（4）新增多行规则行，点击<排序>按钮，上下拖动列表前 ≡ 符号可改变规则行上下顺序。



（5） 点击<删除>按钮，点击列表前 − 符号可删除规则行。



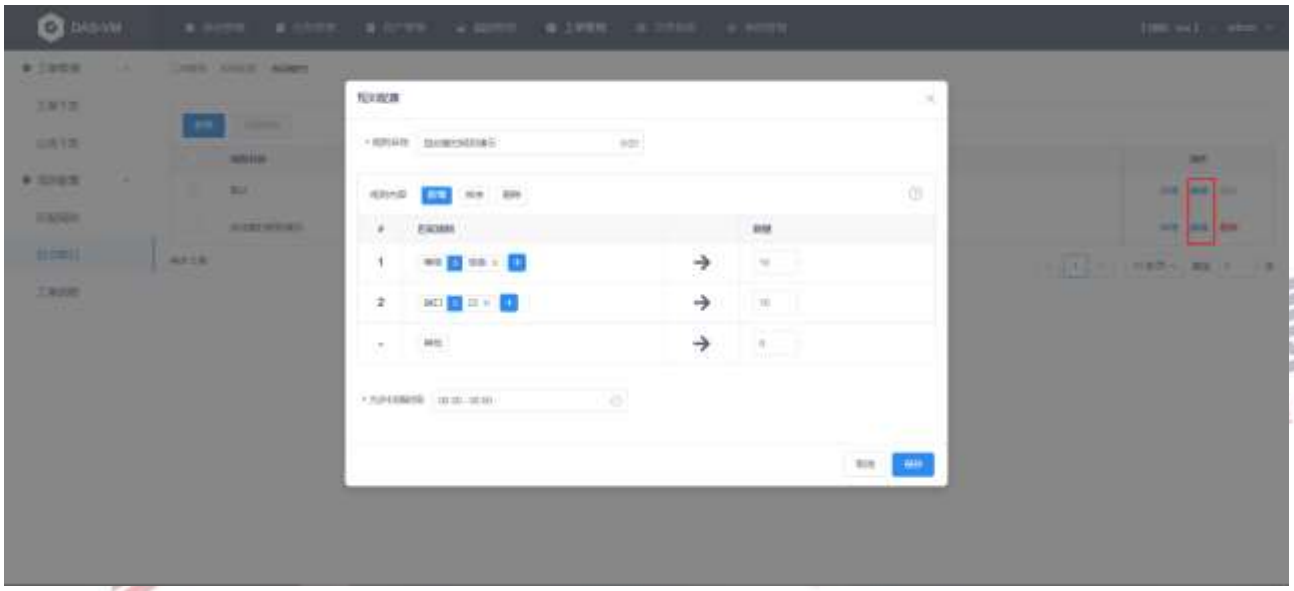
（6） 选择允许扫描时段后，点击<保存>按钮，即可新增新的自动复扫规则。



7.2.2.2. 编辑自动复扫规则

（1） 点击自动复扫规则列表的<详情>按钮，可查看自动复扫规则的详细内容。

（2） 点击自动复扫规则列表的<编辑>按钮，在编辑规则配置窗口，修改规则名称、规则条件和允许扫描时段。点击<新增>按钮新增规则行，点击 + 符号下拉选择匹配内容、条件并输入值，点击<确定>按钮，选择指定人员类型即可完成单条规则创建；点击<删除>按钮，点击列表前 − 符号可删除规则行；点击<排序>按钮，上下拖动列表前 ≡ 符号可改变规则行上下顺序；点击<保存>按钮即可完成自动复扫规则的编辑



7.2.2.3. 默认自动复扫规则

（1） 点击自动复扫规则列表规则名称后的<设为默认>按钮，即可将该规则设置为默认自动复扫规则，工单创建时默认优先选择默认自动复扫规则。

7.2.2.4. 删除自动复扫规则

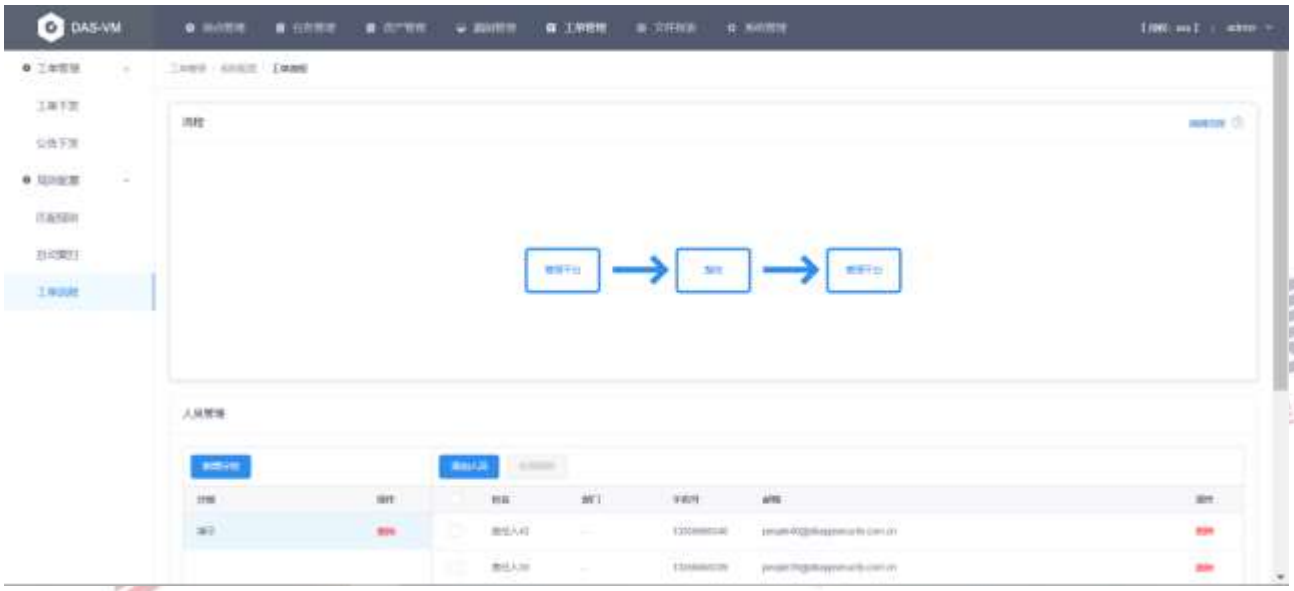
（1） 点击自动复扫规则列表的<删除>按钮并确认，即可删除相应自动复扫规则；默认自动复扫规则无法删除。

7.2.3. 工单流程

用于自定义工单流转各节点的流程及各节点的人员权限。

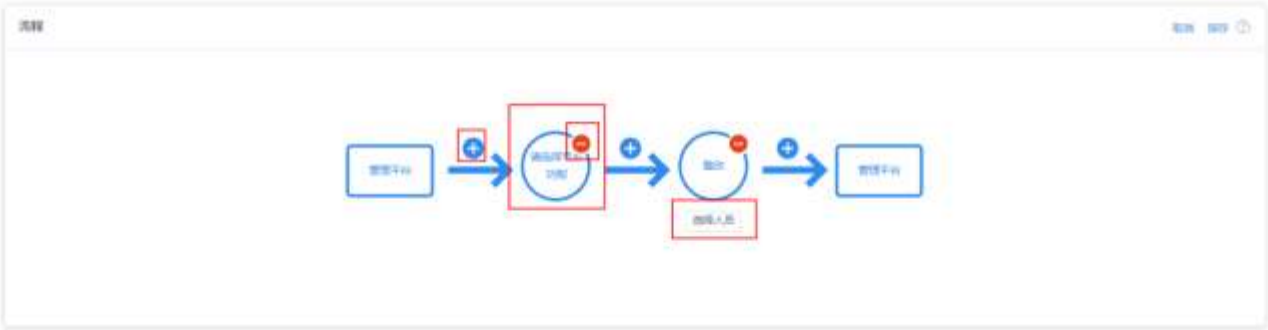
7.2.3.1. 编辑工单流程

（1） 用户 WEB 登录后，进入[工单管理 /规则配置/工单流程]页面。出厂默认工单流程为：管理平台-整改-管理平台。

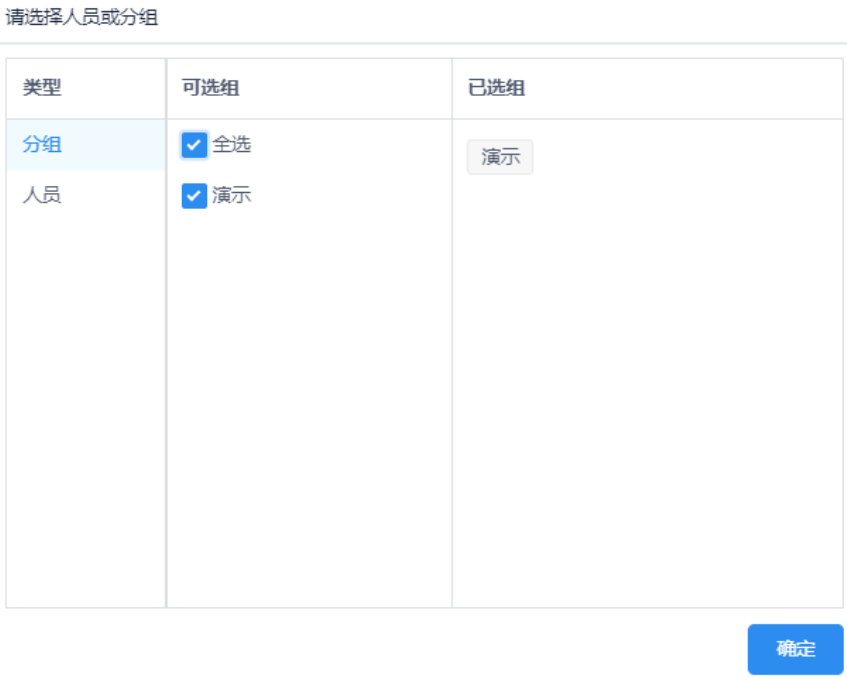


（2）点击<编辑流程>按钮，进入编辑流程页面。

（3）点击 符号增加节点；点击<请选择节点功能>按钮选择节点功能，节点功能包括分发、整改和审核，首个节点不能为审核，最后一个节点不能为分发；点击 符号可删除对应节点。工单流程中至少包含一个整改节点。



（4）点击<选择人员>按钮选择拥有该节点权限的工单系统人员， 点击类型列下<分组>勾选可选组进行批量人员选择，也可点击类型列下<人员>勾选可选人员进行逐个人员选择，点击<确定>完成人员选择。



（5） 点击<取消>按钮取消本次工单流程的编辑，编辑不生效；，点击<保存>按钮完成本次工单流程的编辑。

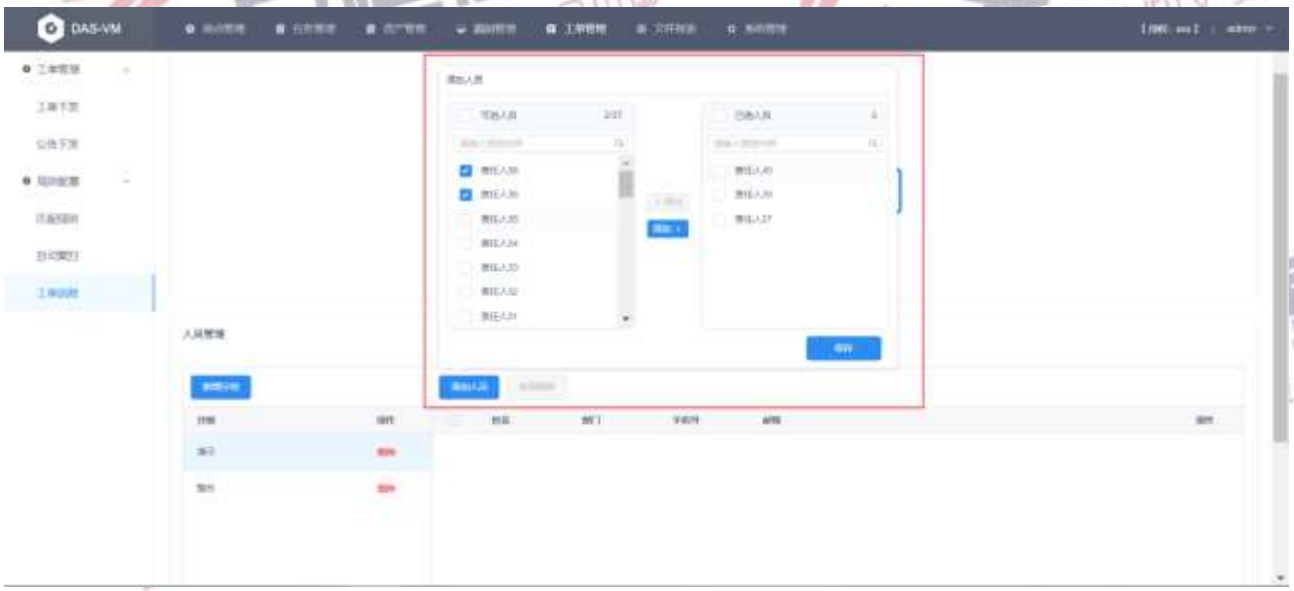
注意

1. 首个节点不允许变更人员，由管理平台自动分配，人员对象为全体责任人。
2. 整个流程中必须存在整改节点，否则无法保存，整改节点只能存在一个。
3. 分发不可作为流程中最后一个节点，审核节点须在整改节点之后。
4. 流程节点仅当全部工单结束（工单状态为已完成或已撤回）时才可进行编辑。
5. 各节点可增加或删除节点责任人，删除责任人仅当全部工单结束（工单状态为已完成或已撤回）时才可进行删除。

7.2.3.2. 分组人员管理

（1） 点击<新增分组>按钮，输入分组名称，点击<确认>按钮创建新分组。

（2）点击<添加人员>按钮，勾选可选人员，点击<添加>按钮选择人员，勾选已选人员，点击<移除>按钮取消选择人员，选择人员完毕后，点击<保存>按钮保存分组已选人员。可通过搜索框搜索指定人员。



（3）若需要删除分组下人员可点击<删除>按钮逐个删除或勾选分组内人员点击<批量删除>按钮进行批量删除。

（4）若需要删除分组可点击分组后<删除>按钮逐个删除。

8. 文件报表

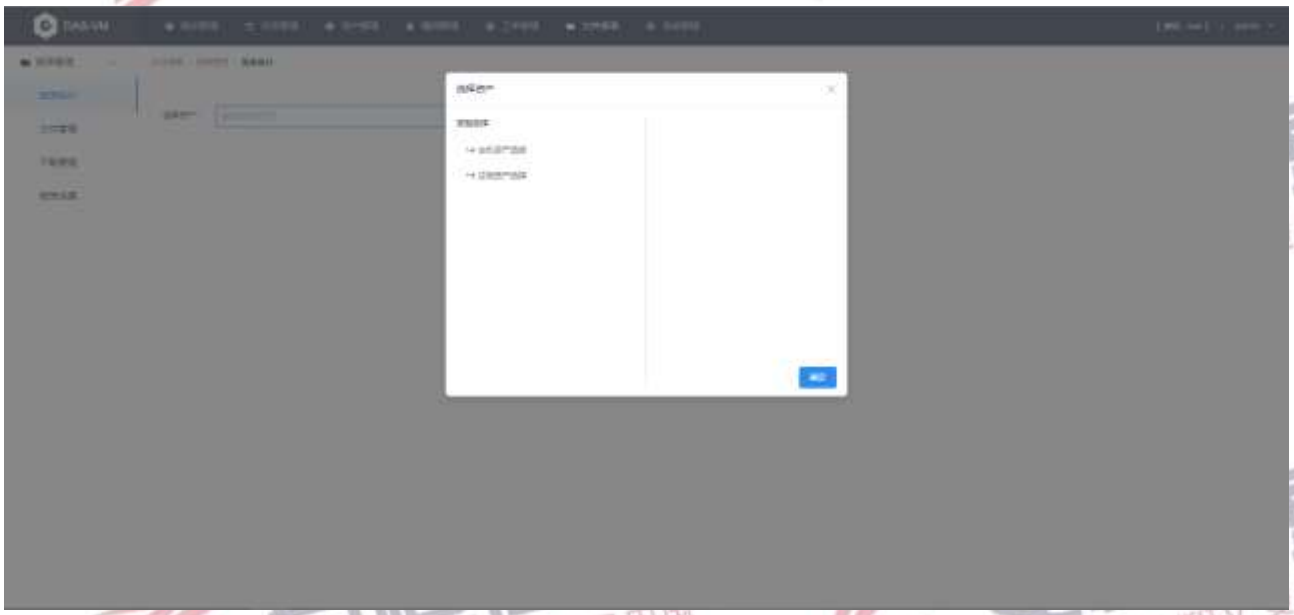
8.1. 报表管理

查看报表统计信息，管理上传的文件和平台导出的报表等文件。

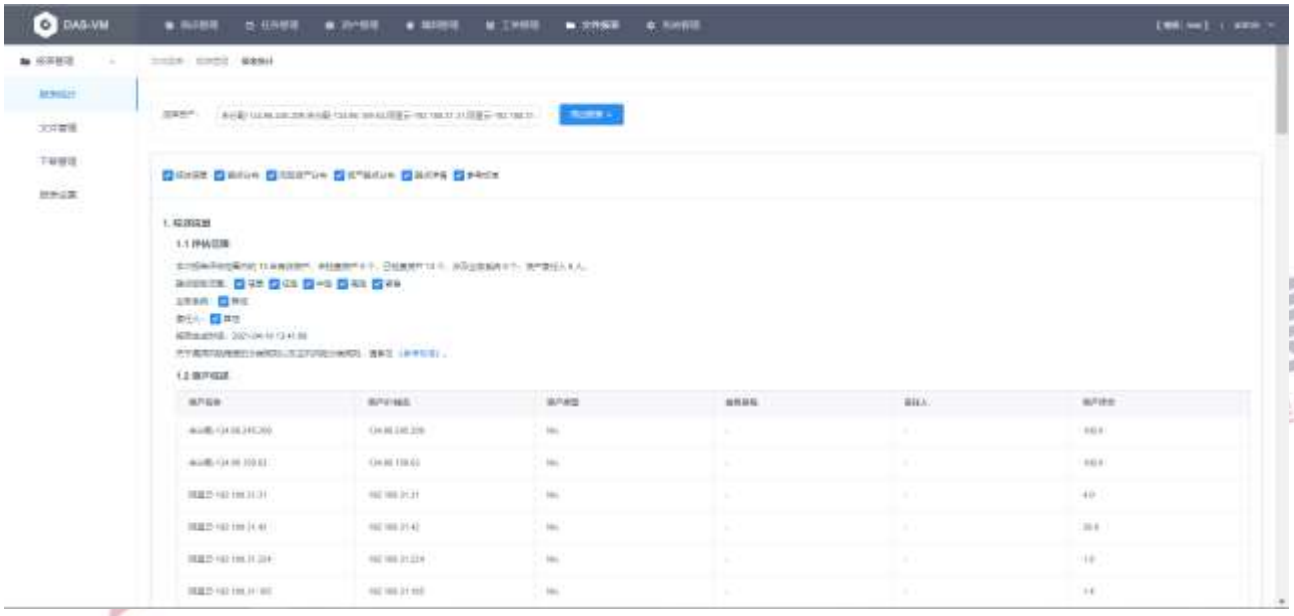
8.1.1. 报表统计

（1） 用户 WEB 登录后，点击进入[文件报表/报表管理/报表统计]页面。

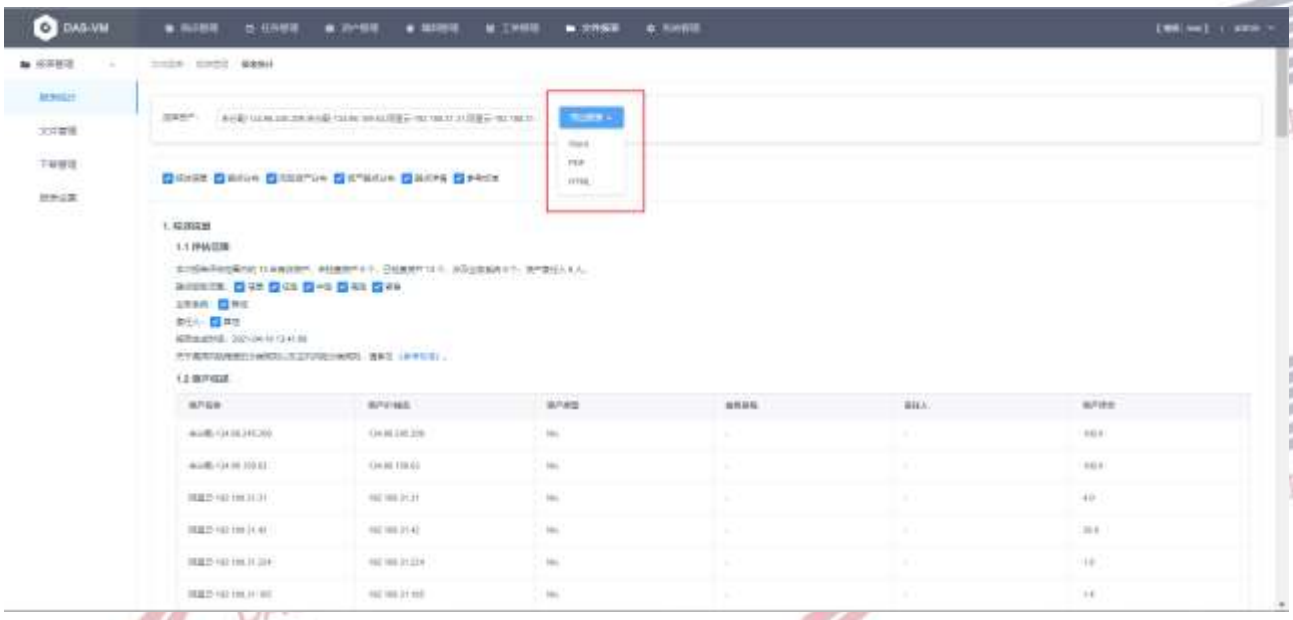
（2） 点击选择资产栏，弹出资产选择窗，选择资产类型，勾选对应资产，点击<确定>按钮。可在查询框输入关键字进行快速资产查询



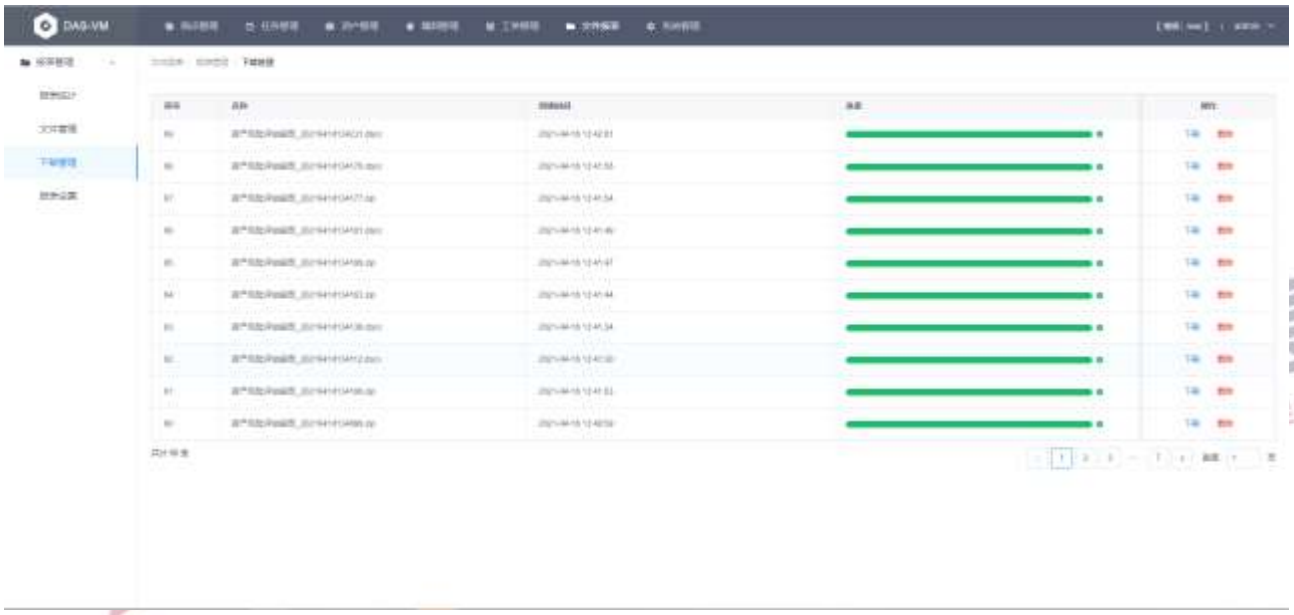
（3） 选择资产后，页面展示选中自查资产的统计报表，包括：综述信息、弱点分布、风险资产分布、资产弱点分布、弱点详情、参考标准等信息，可选择报表生成内容、弱点级别范围、业务系统和责任人。



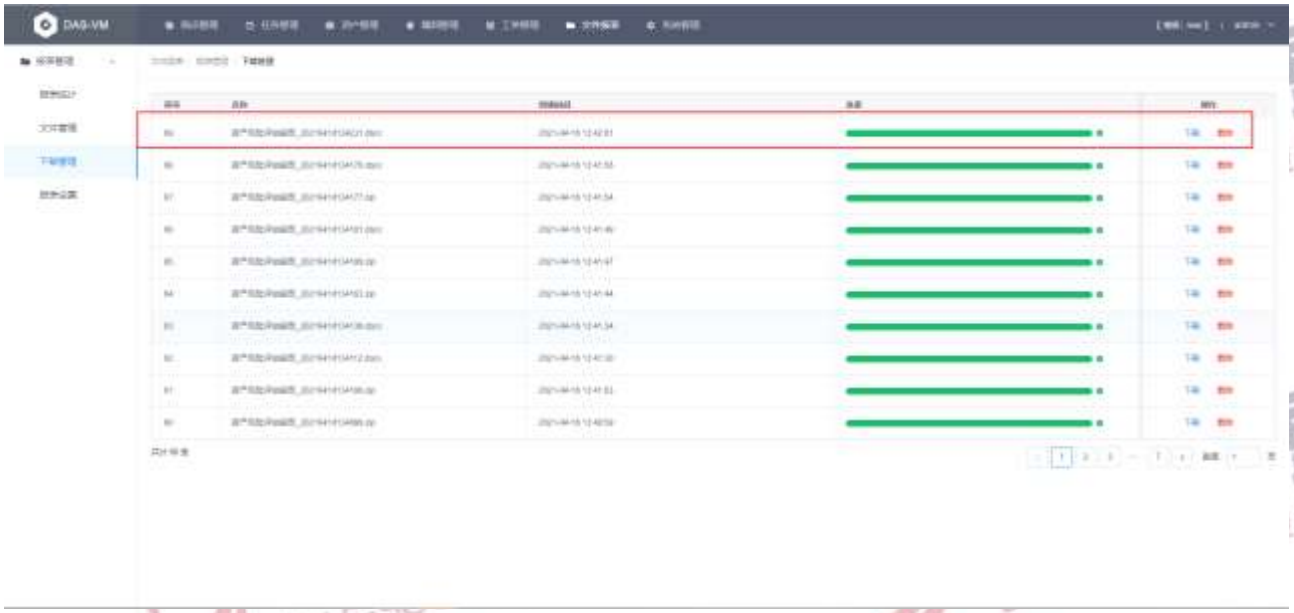
（4） 点击选择资产栏后的<导出报表>按钮，下拉展开导出格式选项，选择导出格式 Word、PDF 或 HTML。



（5） 新打开一个标签页并进入到[文件报表/报表管理/下载管理]页面，下载管理列表新增一条导出记录，并显示导出报表进度。



（6） 待进度条达到 100%转绿后，点击<下载>按钮，下载导出的资产风险评估报告。

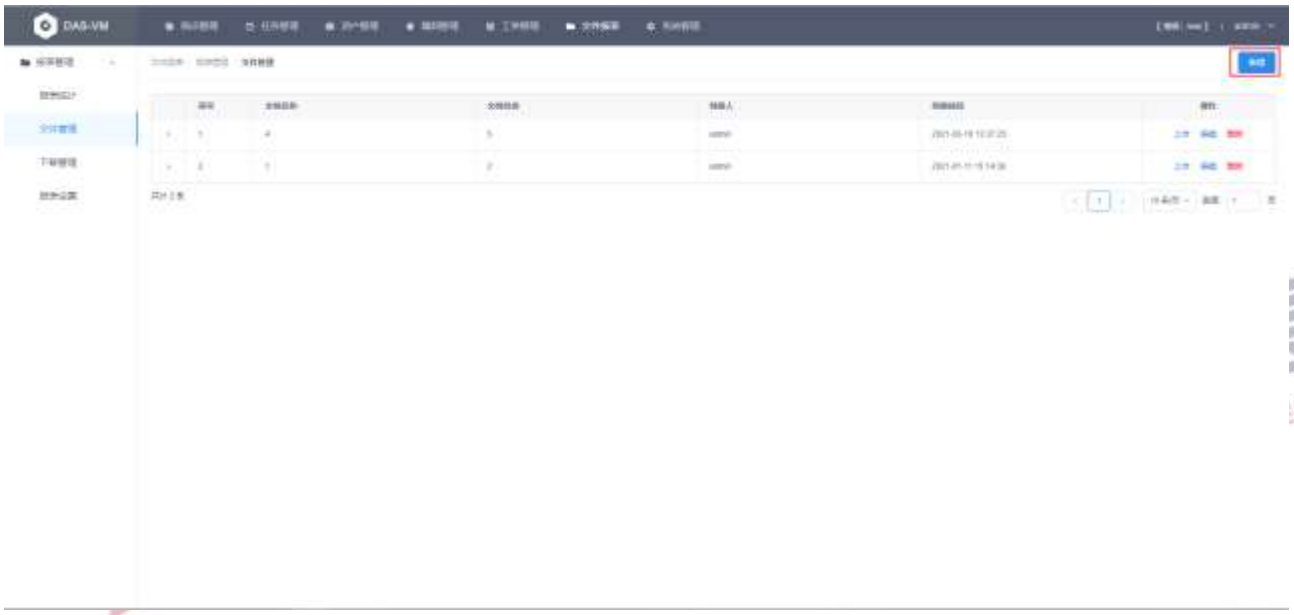


8. 1. 2. 文件管理

8. 1. 2. 1. 新增文档

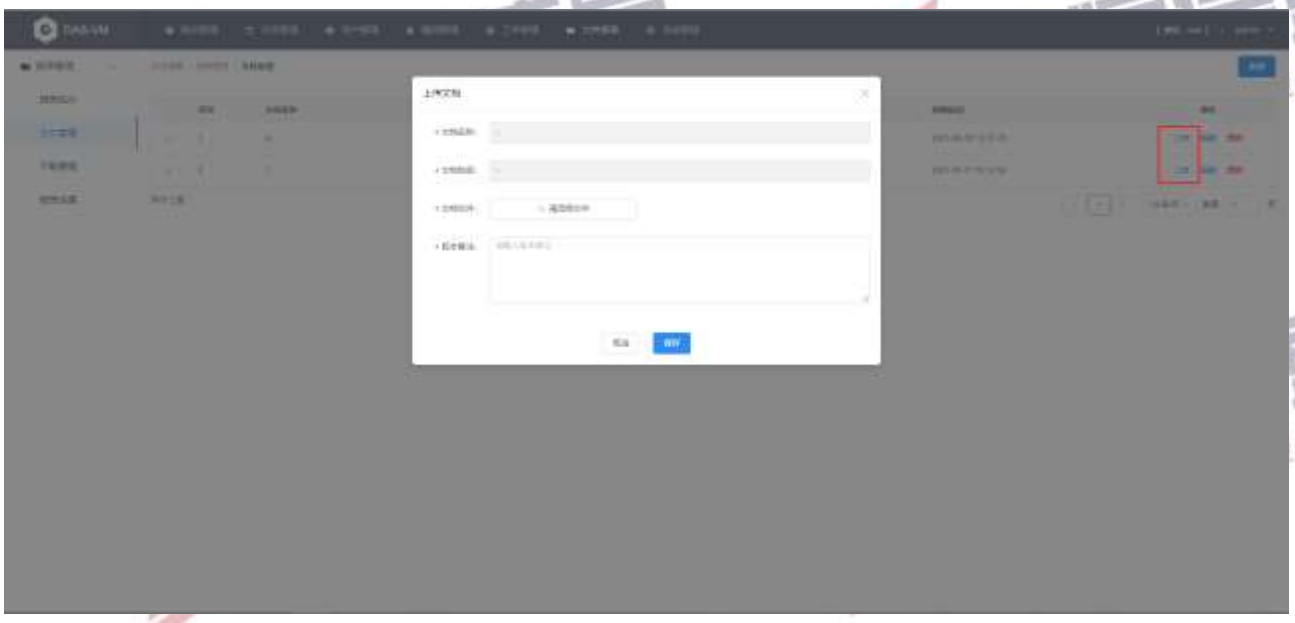
（1） 用户 WEB 登录后，进入[文件报表/报表管理/文件管理]页面。

（2） 点击<新增>按钮，进入新增文档页面，填写对应的文档信息，选择文件，点击<保存>按钮，文档列表新增相应文档。



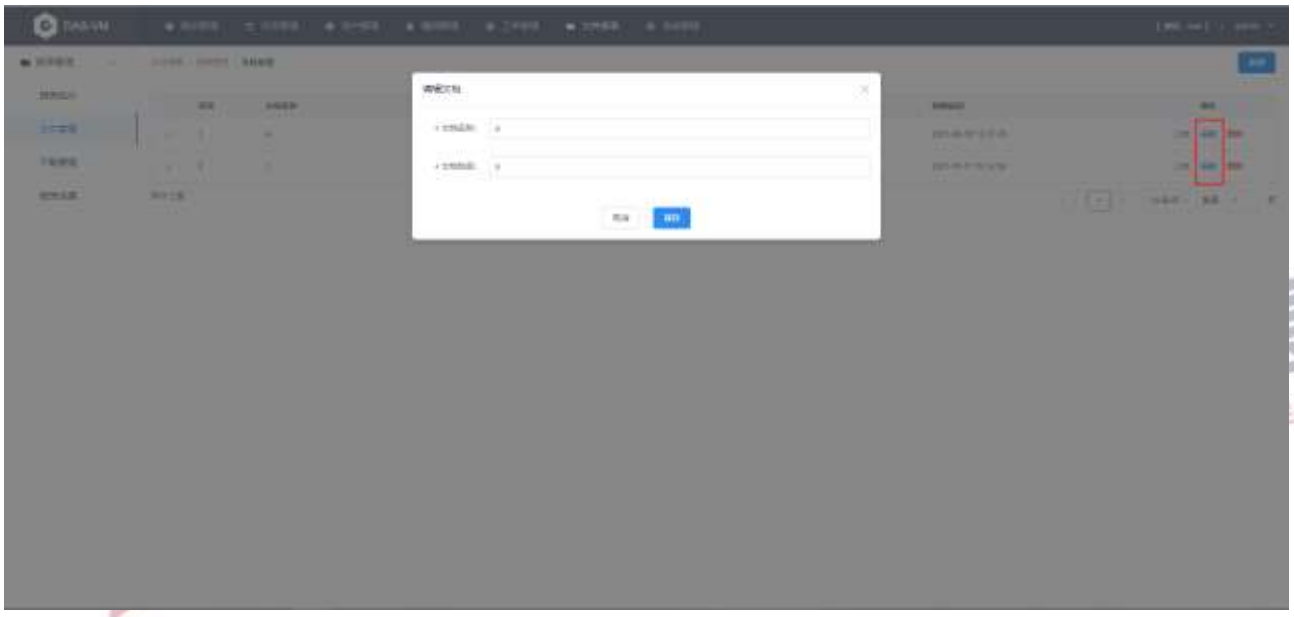
8.1.2.2. 上传文档

（1） 点击文档列表中的<上传>按钮，弹出上传文档窗口，选择文件并输入版本备注，点击<保存>按钮，可再次上传文件至列表中的相应文档。



8.1.2.3. 编辑文档

（1） 点击文档列表中的<编辑>按钮，弹出编辑文档窗口，修改文档名称和文档性质，点击<保存>按钮，可编辑列表中的相应文档。



8.1.2.4. 删除文档

（1） 点击文档列表中的<删除>按钮并却确定，可删除列表中的相应文档。

8.1.2.5. 下载子文档

（1） 点击文档列表中的下拉选项，展开子文档列表。点击子文档列表中的<下载>按钮，可下载对应子文档。

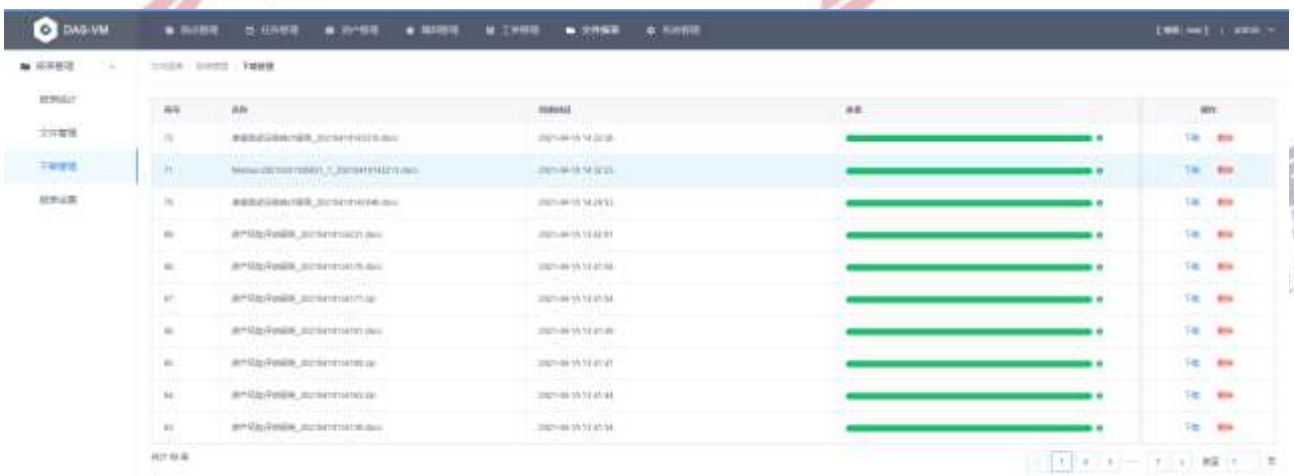
8.1.2.6. 删除子文档

（1） 点击子文档列表中的<删除>按钮并确定，可以删除列表中的相应子文档。

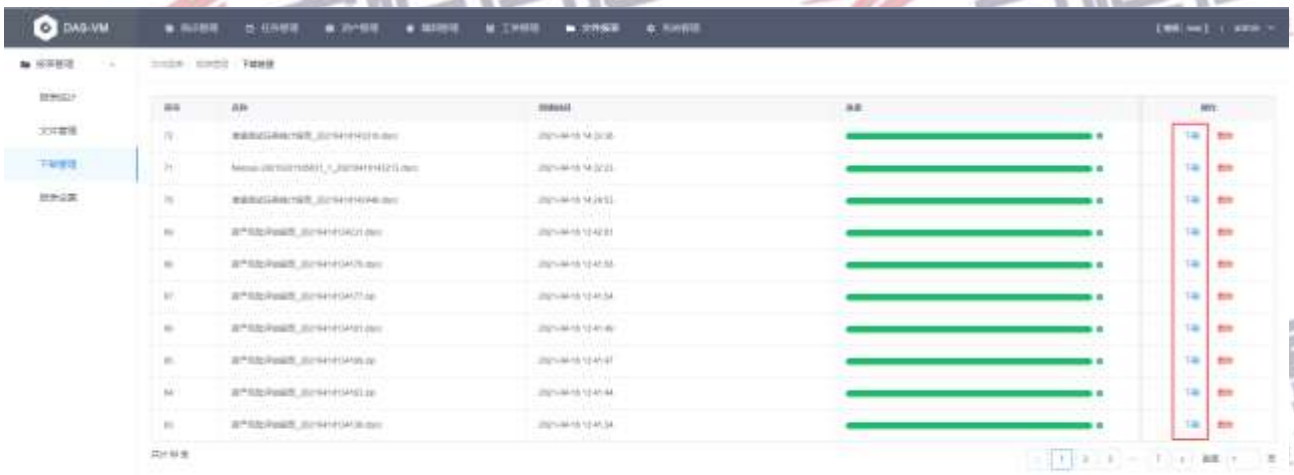
8.1.3. 下载管理

8.1.3.1. 下载报表

（1） 用户 WEB 登录后，进入[文件报表/报表管理/下载管理]页面。

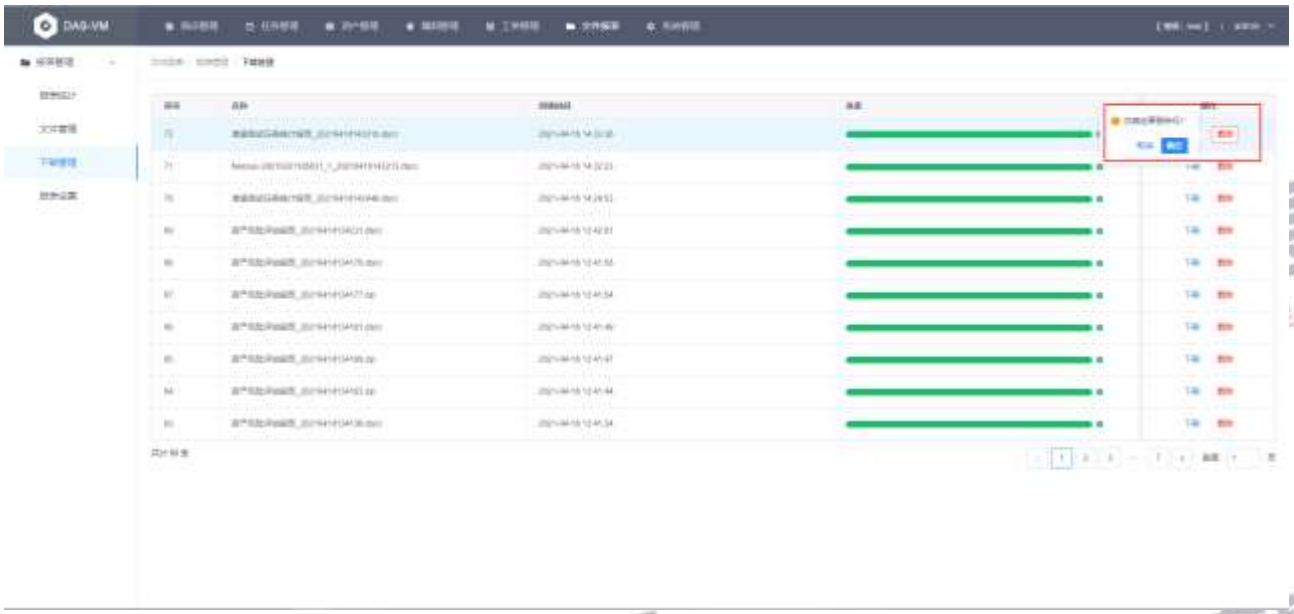


（2） 点击下载列表中的<下载>按钮，可以下载列表中的相应报表。



8.1.3.2. 删除报表

（1） 点击下载列表中的<删除>按钮并确定，可删除列表中的相应统计报表。



8.1.4. 报表设置

（1） 用户 WEB 登录后，进入[文件报表/报表管理/报表设置]页面。选择默认报表生成内容和默认等级范围，完成选择后点击<保存>按钮。

9. 系统管理

9.1. 平台管理

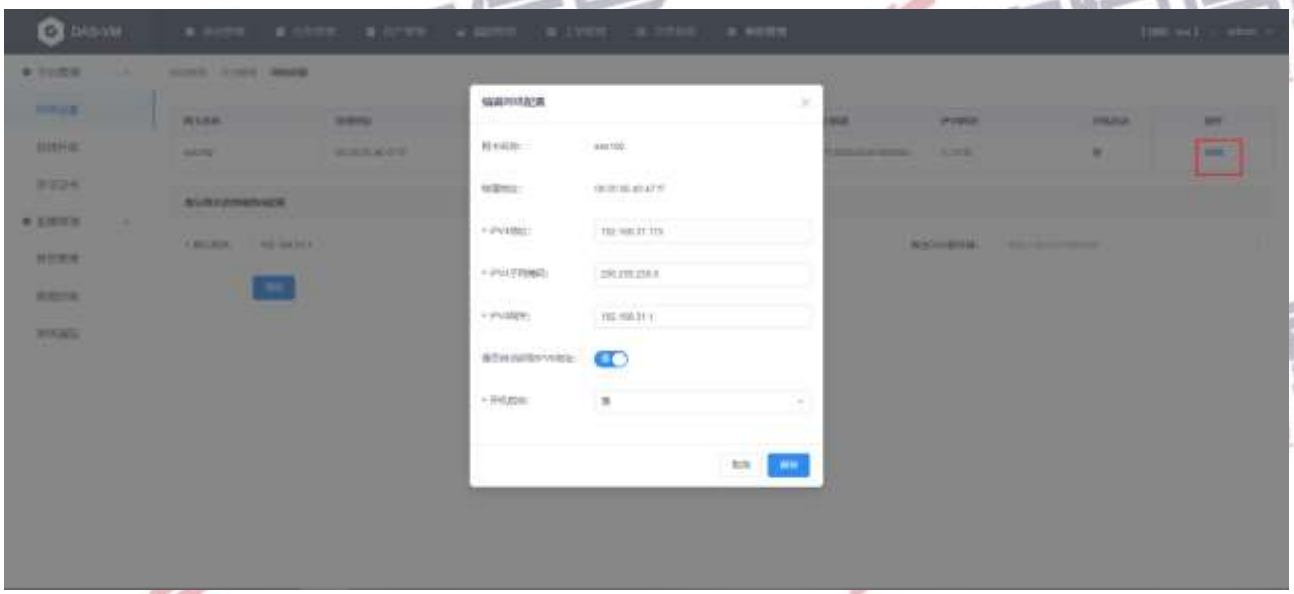
主要用于网络配置、在线升级与许可授权。

9.1.1. 网络设置

9.1.1.1. 网卡配置

（1） 用户 WEB 登录后，进入[系统管理/平台管理/网络设置]页面。

（2） 点击网卡列表的<编辑>按钮，弹出网卡配置编辑窗口，修改网卡相关信息，并点击<确定>按钮，保存配置。



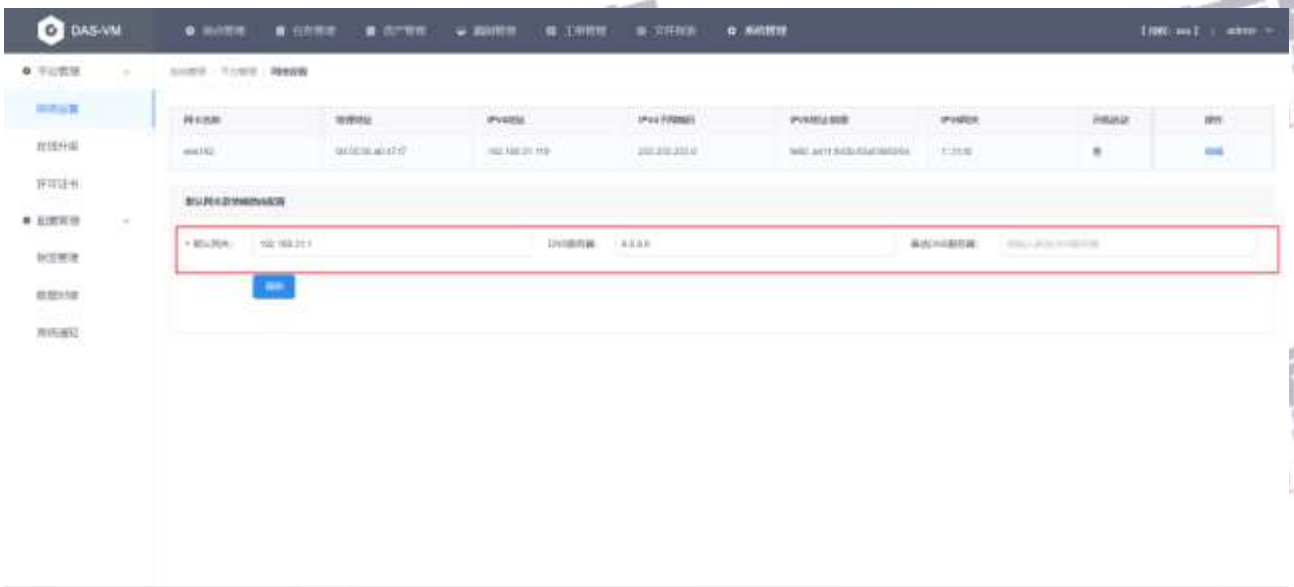
网卡配置配置项及说明见下表：

配置项	说明
网卡名称	对应 ifconfig 的网卡名称
物理地址	该网卡的 mac 地址
IPV4 地址	该网卡配置的 IP 地址
IPV4 子网掩码	该网卡的 IPV4 子网掩码信息

IPV4 网关	该网段的网关信息
是否自动获取 IPV6 地址	是否自动获取 IPV6 地址，选项分为是和否 是：自动分配 IPV6 地址 否：可手工配置 IPV6 地址、IPV6 前缀和 IPV6 网关
IPV6 地址	该网卡配置的 IPV6 地址
IPV6 前缀	该网卡配置的 IPV6 前缀
IPV6 网关	该网段的 IPV6 网关信息
开机启动	是否开机自启动显示

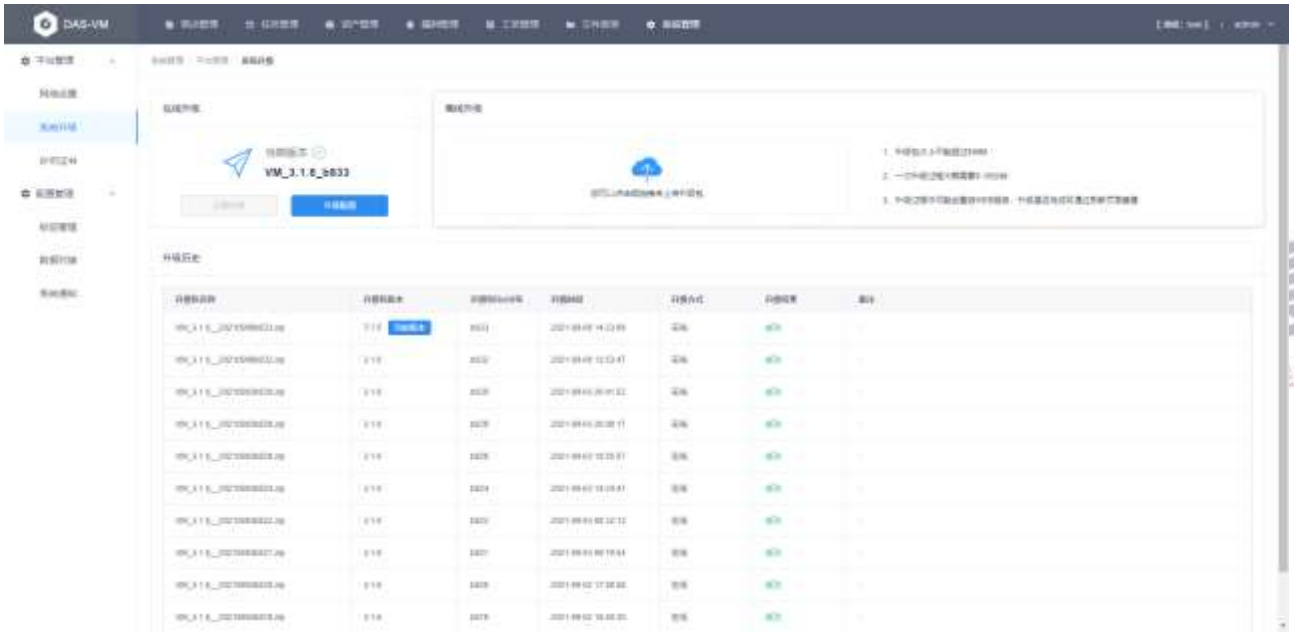
9.1.1.2. 默认网关配置

（1） 默认网关栏修改默认网关、DNS 服务器和备选 DNS 服务器，点击<保存>按钮，保存网关配置。默认网关为必填项。



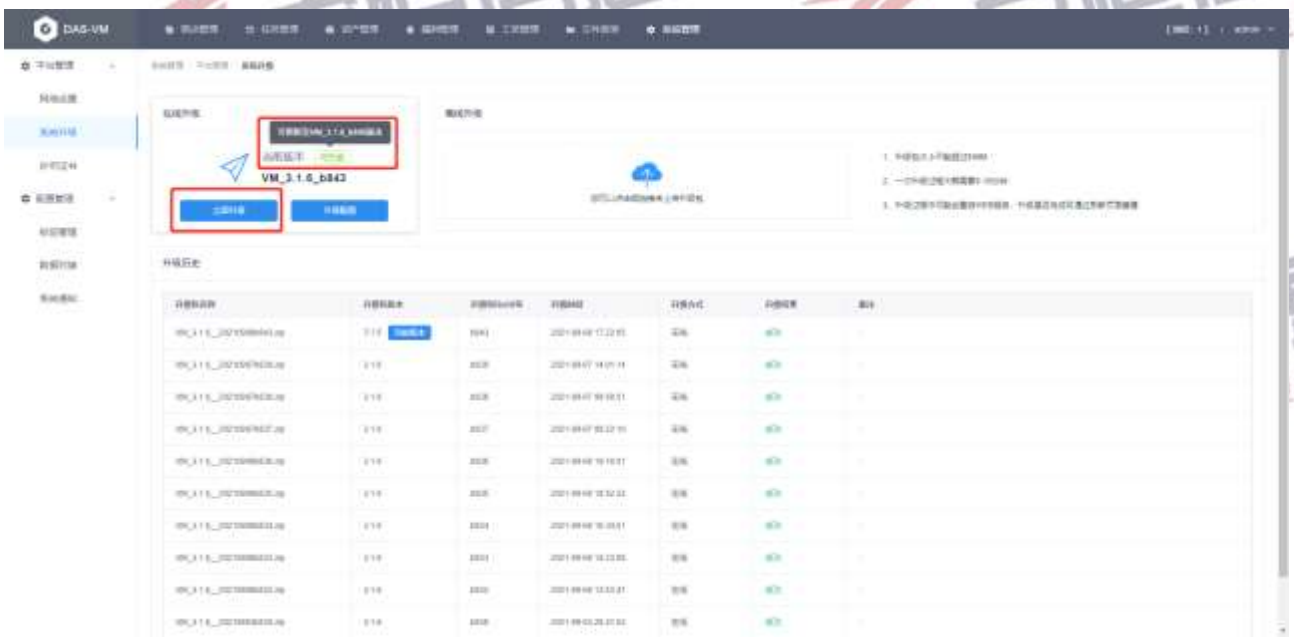
9.1.2. 系统升级

（1） 用户 WEB 登录后，进入[系统管理/平台管理/系统升级]页面，查看升级历史，包含升级包名称、升级包版本、升级包 Build 号、升级时间、升级方式、升级结果以及备注，可由当前版本的最新安装包升级到下一个版本的系统。

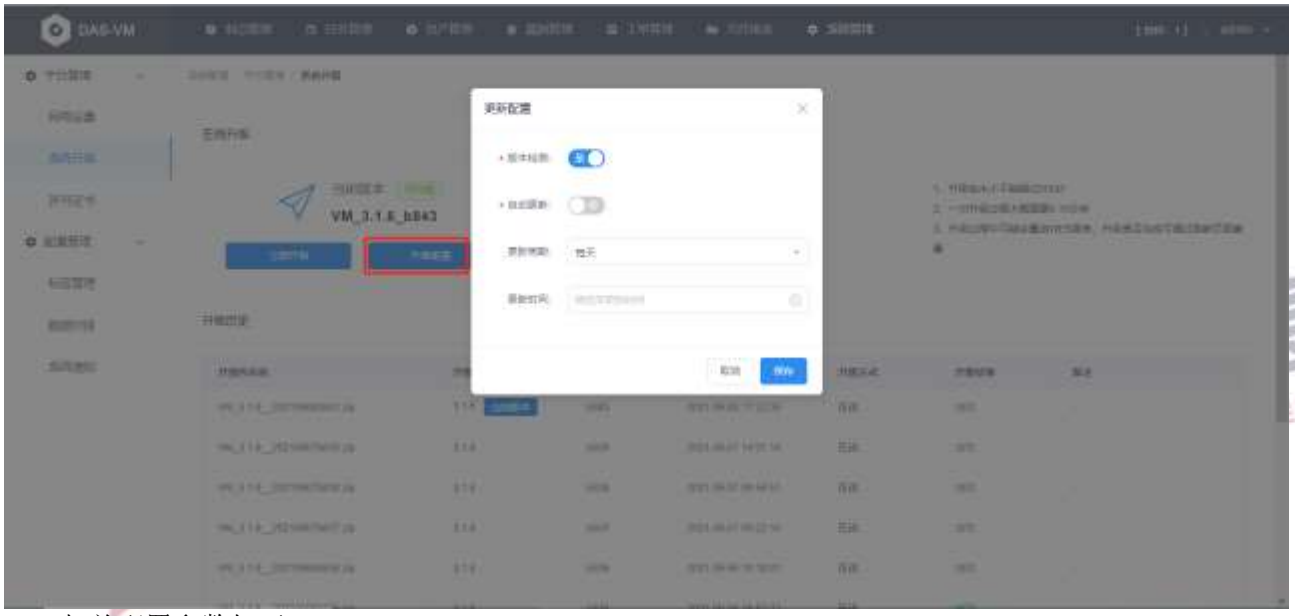


9.1.2.1. 在线升级

（1） 当系统存在可升级的新包，在系统升级-在线升级部分中会显示可升级，点击<立即升级>按钮可以进行升级。



（2）在系统升级-在线升级部分中，点击<升级配置>，更新配置。

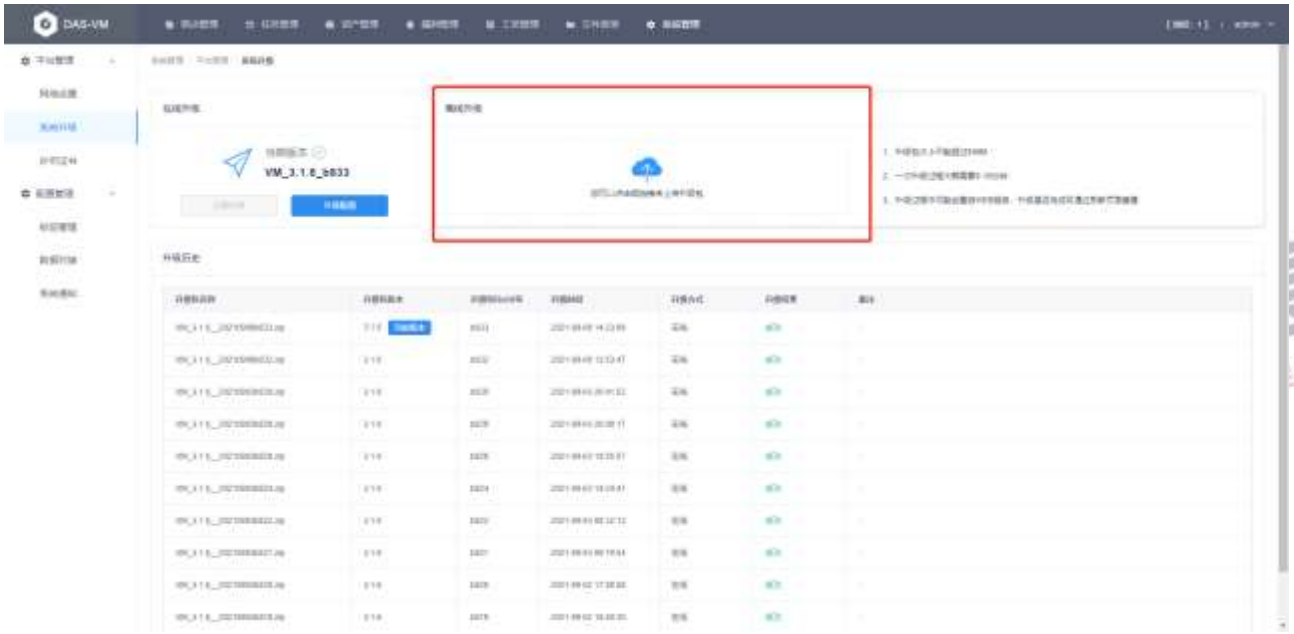


相关配置参数如下：

配置项	说明
版本检测	必选项。选择是否进行版本检测。
自动更新	必选项。选择是否自动更新。
更新周期	选填项。选择更新周期。
更新时间	选填项。选择更新时间。

9.1.2.2. 离线升级

（1） 点击<您可以点击或拖拽来上传升级包>按钮所在框，弹出文件选择窗口选择升级包，或直接拖曳文件至上传框，上传升级包可以对系统进行在线升级，会出现进度条展示示升级包文件的上传进度。



（2）进度条到达 100%后，表示上传完成，系统进行自动升级。自动更新中系统将无法访问，请耐心等待，大概 5 分钟时间，系统会自动跳转到登录页面，表示升级完成。

9.1.3. 许可证书

（1）用户 WEB 登录后，进入[系统管理/平台管理/许可证书]页面，查看许可信息。

（2）点击<更新证书>按钮 ，弹出许可更新窗口，点击<请选择文件>或<导入>按钮选择正确的许可文件上传即可更新证书。

（3） 点击<导出申请文件>或<导出>按钮可下载对应的许可申请文件。

9.2. 配置管理

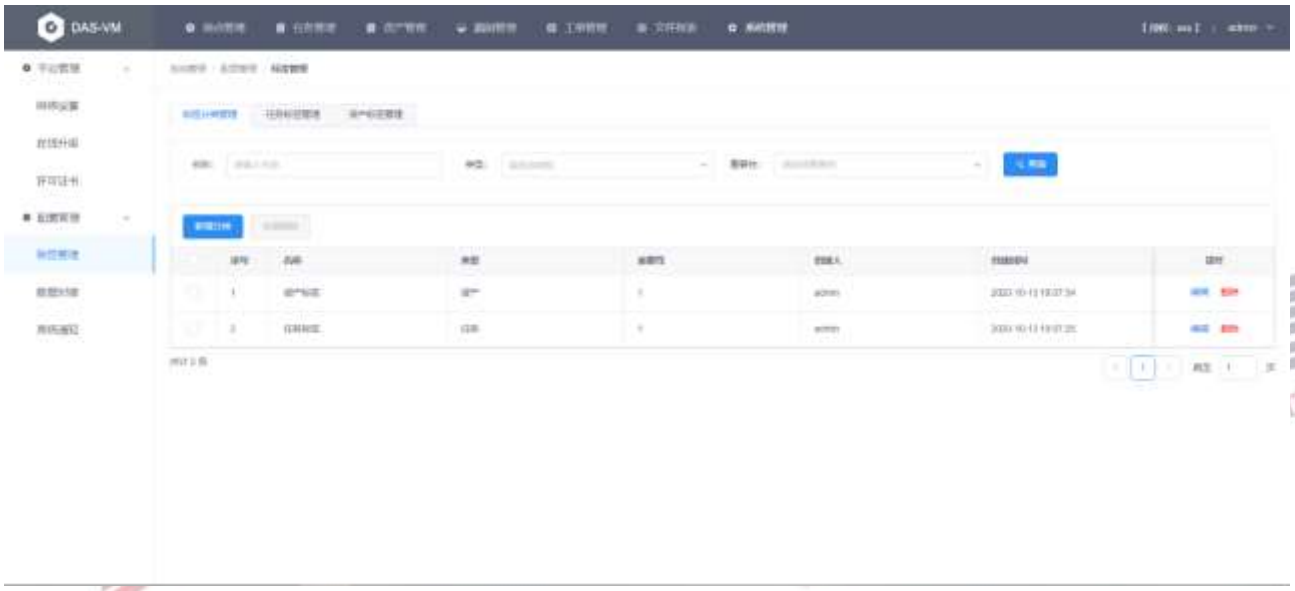
配置管理主要用于进行一些平台的系统配置，包括：扫描引擎管理、偏好设置、标签管理和信息维护

9.2.1. 标签管理

标签管理页面主要用于对标签分类、任务标签和资产标签的增、删、改、查等管理。

9.2.1.1. 标签分类管理

（1） 用户 WEB 登录后，进入[系统管理/配置管理/标签管理]页面，默认显示标签分类管理 tab 页。



（1）新增标签分类

点击<新增分类>按钮，弹出新增标签分类窗口，填写相应的配置项信息，点击<保存>按钮，即可完成标签分类添加。

标签分类配置项及说明见下表：

配置项	说明
名称	必填项。填写标签类名称
类型	必填项。设置标签类型，包括：任务和资产
重要性	选填项。标记此分类的重要程度，分为 1-10
创建人	默认当前登录用户名，置灰，不可更改

（2）编辑标签分类

点击标签分类列表中的<编辑>按钮，弹出编辑标签分类窗口，编辑相应的配置项信息，点击<保存>按钮，即可完成标签分类修改。类型与创建人不可编辑。

（3）删除标签分类

点击标签分类列表中的<删除>按钮并确定，即可删除对应标签分类。或勾选多个标签后，点击标签分类列表上面的<批量删除>按钮并确定，即可批量删除选中的标签分类。

（4）查询标签分类

查询栏输入查询条件，点击<查询>按钮，即可查询标签分类。

9.2.1.2. 任务标签管理

（1） 用户 WEB 登录后，进入[系统管理/配置管理/标签管理]的任务标签管理 tab 页。

（1）新增任务标签

点击<新增标签>按钮，弹出新增任务标签窗口，填写相应的配置项信息，点击<保存>按钮，即可完成任务标签添加。

任务标签配置项及说明见下表：

配置项	说明
名称	必填项，填写任务标签名称
类型	必填项，设置任务标签所属任务分类标签，可选择标签分类里添加的任务分类标签
重要性	标记此任务标签的重要程度，分为 1-10
创建人	默认当前登录用户名，置灰，不可更改

（2）编辑任务标签

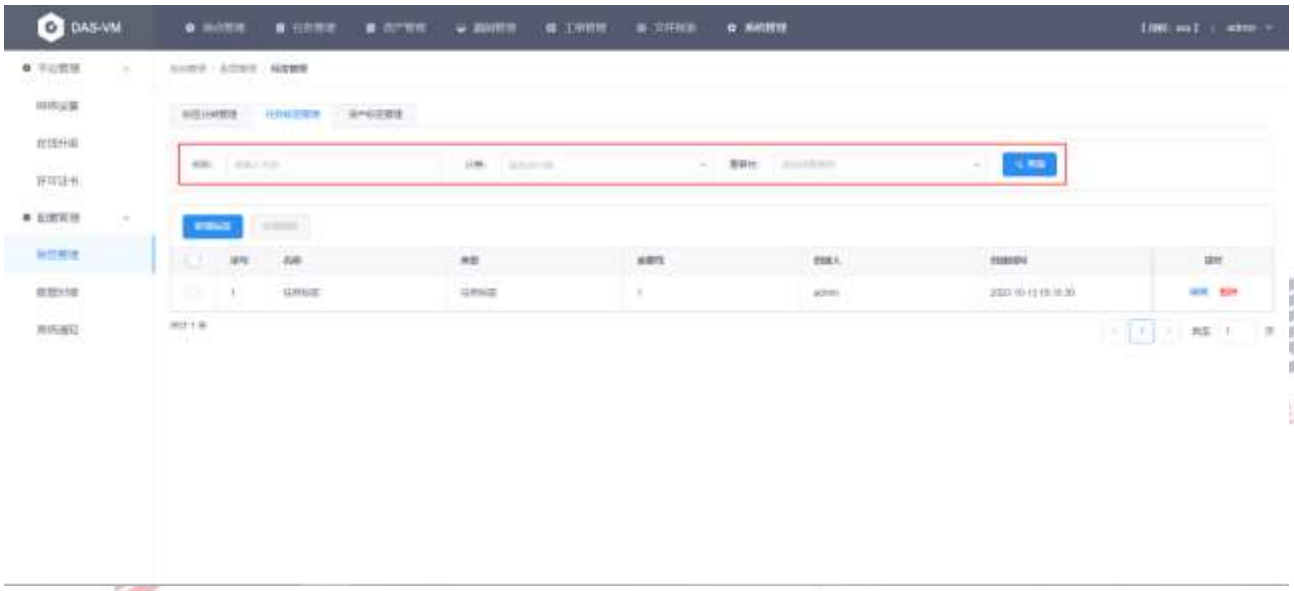
点击任务标签列表中的<编辑>按钮，弹出编辑任务标签窗口，编辑相应的配置项信息，点击<保存>按钮，即可完成任务标签修改。创建人不可编辑。

（3）删除任务标签

点击任务标签列表中的<删除>按钮并确定，即可删除对应任务标签。或勾选多个标签后，点击任务标签列表上面的<批量删除>按钮并确定，即可批量删除选中的任务标签。

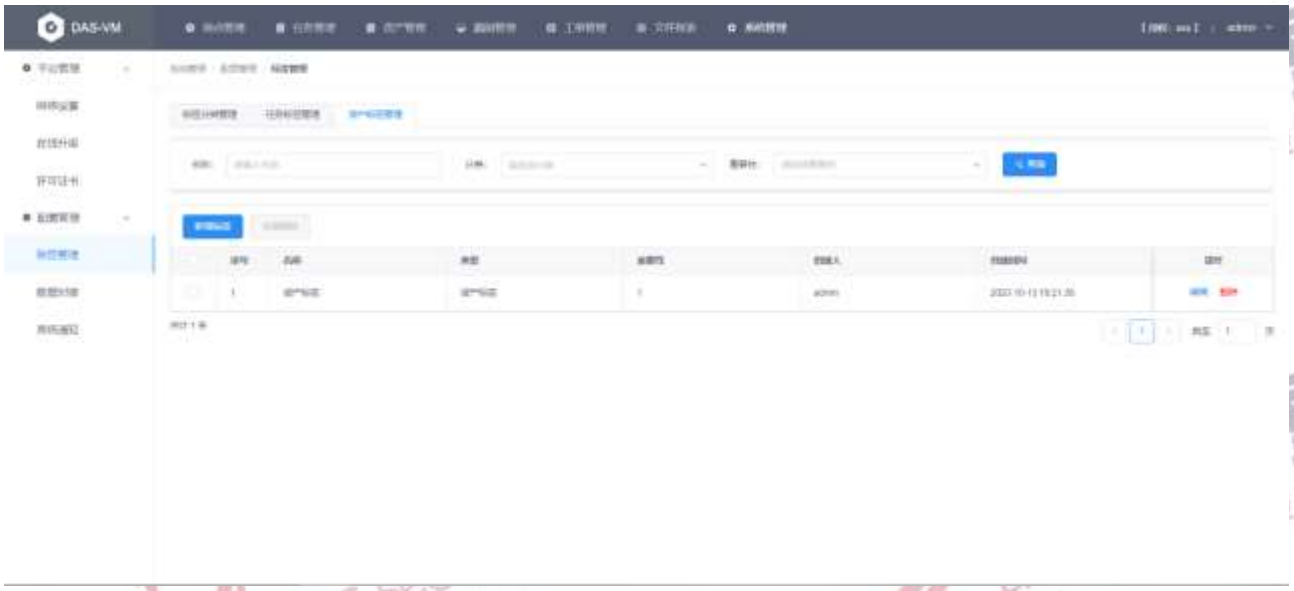
（4）查询任务标签

查询栏输入查询条件，点击<查询>按钮，即可查询任务标签。



9.2.1.3. 资产标签管理

（1） 用户 WEB 登录后，进入[系统管理/配置管理/标签管理]的资产标签管理 tab 页。



（1）新增资产标签

点击<新增标签>按钮，弹出新增资产标签窗口，填写相应的配置项信息，点击<保存>按钮，即可完成资产标签添加。

资产标签配置项及说明见下表：

配置项	说明
名称	必填项。填写资产标签名称
类型	必填项。设置资产标签所属资产分类标签，可选择标签分类里添加的资产分类标签
重要性	选填项。标记此资产标签的重要程度，分为 1-10
创建人	默认当前登录用户名，置灰，不可更改

（2）编辑资产标签

点击资产标签列表中的<编辑>按钮，弹出编辑资产标签窗口，编辑相应的配置项信息，点击<保存>按钮，即可完成资产标签修改。创建人不可编辑。

（3）删除资产标签

点击资产标签列表中的<删除>按钮并确定，即可删除对应资产标签。或勾选多个标签后，点击资产标签列表上面的<批量删除>按钮并确定，即可批量删除选中的资产标签。

（4）查询资产标签

查询栏输入查询条件，点击<查询>按钮，即可查询资产标签。

9.2.2. 数据对接

数据对接主要是对接大数据平台的数据端口。

9.2.2.1. 大数据平台

（1） 用户 WEB 登录后，进入[系统管理/配置管理/数据对接]页面，默认显示大数据平台 tab 页。

（2） 填写大数据平台对接配置参数。

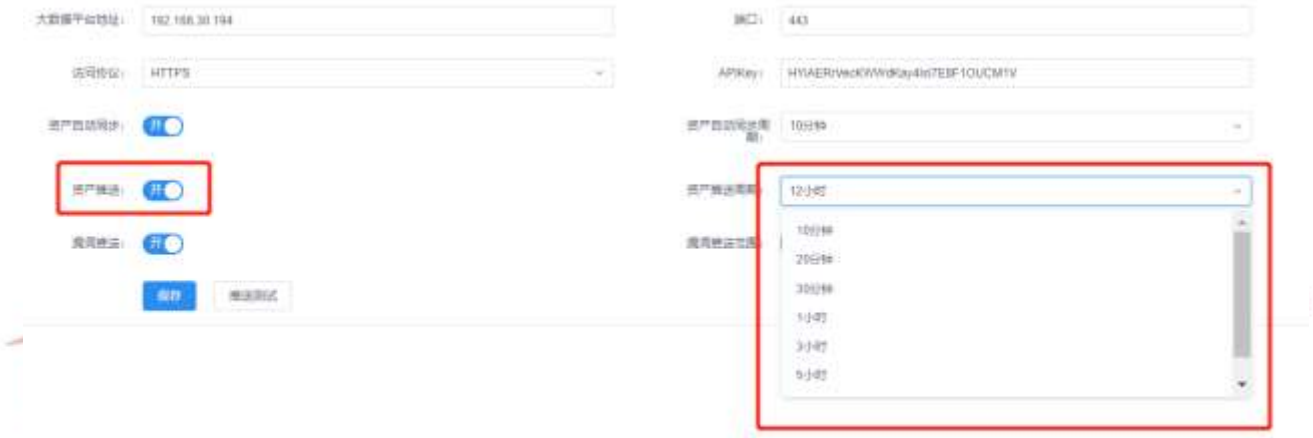
大数据平台配置参数说明见下表：

配置项	说明
大数据平台地址	大数据平台的页面登录 IP。
端口	大数据平台页面访问地址的端口。
访问协议	大数据平台页面访问地址的协议，可选 http 或 https。
APIKey	大数据平台的接口调用 APIKEY，一般为默认值，无需修改。
资产自动同步	从大数据平台获取资产类型、名称填充至弱点平台（仅会获取当前弱点平台存在的 IP 资产信息）。
资产自动同步周期	资产信息同步周期，周期资产同步在保存配置时立即同步一次，此后在上一次周期同步的结束时间基础上增加周期时间作为下一次周期同步的开始时间。
资产推送	向大数据平台推送资产。支持周期全量资产推送和扫描结束时推送扫描发现的资产结果。
资产推送周期	资产推送周期，期全量资产推送功能在保存配置时立即推送一次，此后在上一次周期推送的结束时间基础上增加周期时间作为下一次周期推送的开始时间。
漏洞推送	扫描结束后向大数据平台推送扫描发现的漏洞结果和资产信息。
漏洞推送范围	可勾选漏洞的推送范围，包括漏洞等级、误报、搁置等，未在勾选范围内的漏洞不进行推送。

（3） 点开<资产自动同步>，可以进行资产自动同步周期配置，该功能可以将大数据平台的资产自动周期同步至弱点管理平台。开启资产同步选项后，周期资产同步在保存配置时立即同步一次，此后在上一次周期同步的结束时间基础上增加周期时间作为下一次周期同步的开始时间，可以设置的资产同步周期有 10 分钟、20 分钟、30 分钟、1 个小时、3 个小时、5 个小时、12 个小时。

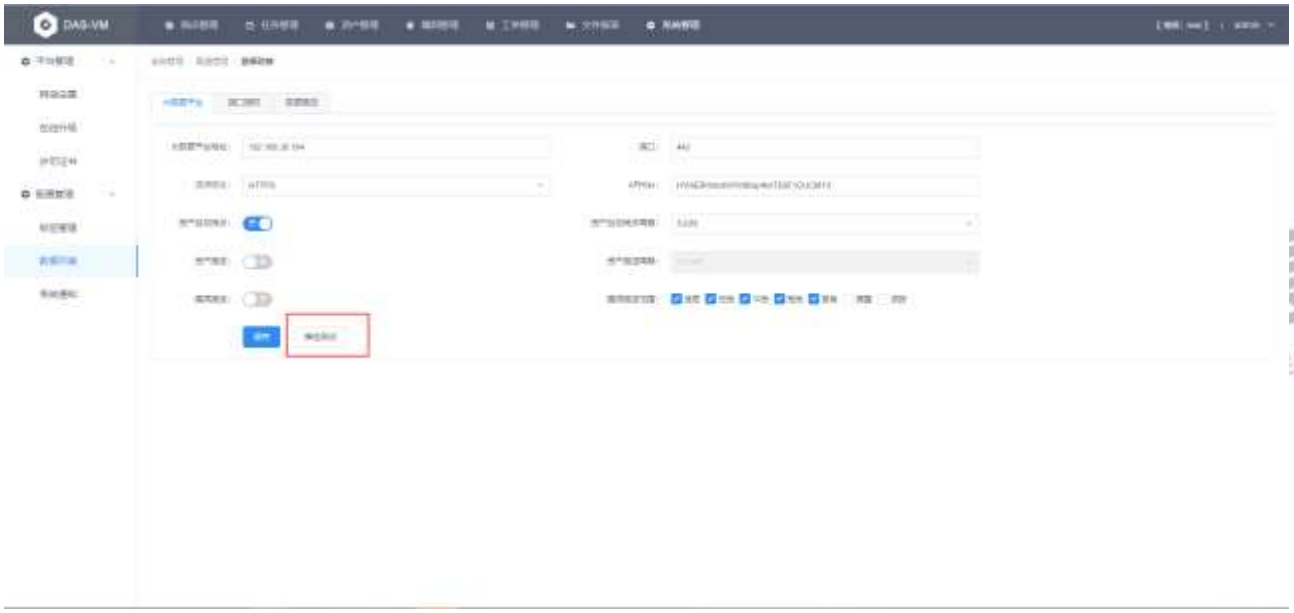
（4） 点开<资产推送>，可以进行资产周期推送，该功能可以向大数据平台快速推送资产，开启资产推送选项后，周期全量资产推送功能在保存配置时立即推送一次，此后在上一次周期推送的结束时

间基础上增加周期时间作为下一次周期推送的开始时间，资产推送周期可手动设置选择 10 分钟、20 分钟、30 分钟、1 个小时、3 个小时、5 个小时、12 个小时。



（5）漏洞推送支持扫描任务结束时推送扫描发现的漏洞结果和资产信息。支持推送漏洞范围自定义，可勾选信息、低危、中危、高危、紧急、搁置、误报等选项，保存后会推送自定义勾选的漏洞。

（6）配置完相关选项后，点击<保存>按钮保存配置，然后点击<推送测试>按钮，后台将推送一条零漏洞数据至指定的大数据平台地址，前端展示返回信息以测试对接是否成功。



注意

在进行大数据平台相关周期同步推送时，需要关闭定时同步推送功能，即击进入[配置管理-数据对接-数据推送]页面后，在资产相关模块中将<定时推送资产>选项关闭，即选择“否”；在任务相关模块中将<扫描结束推送漏洞>和<发现资产时推送资产>选项关闭，即选择“否”。

9.2.2.2. 接口授权

（1） 用户 WEB 登录后，进入[系统管理/配置管理/数据对接]页面的接口授权 tab 页。

2

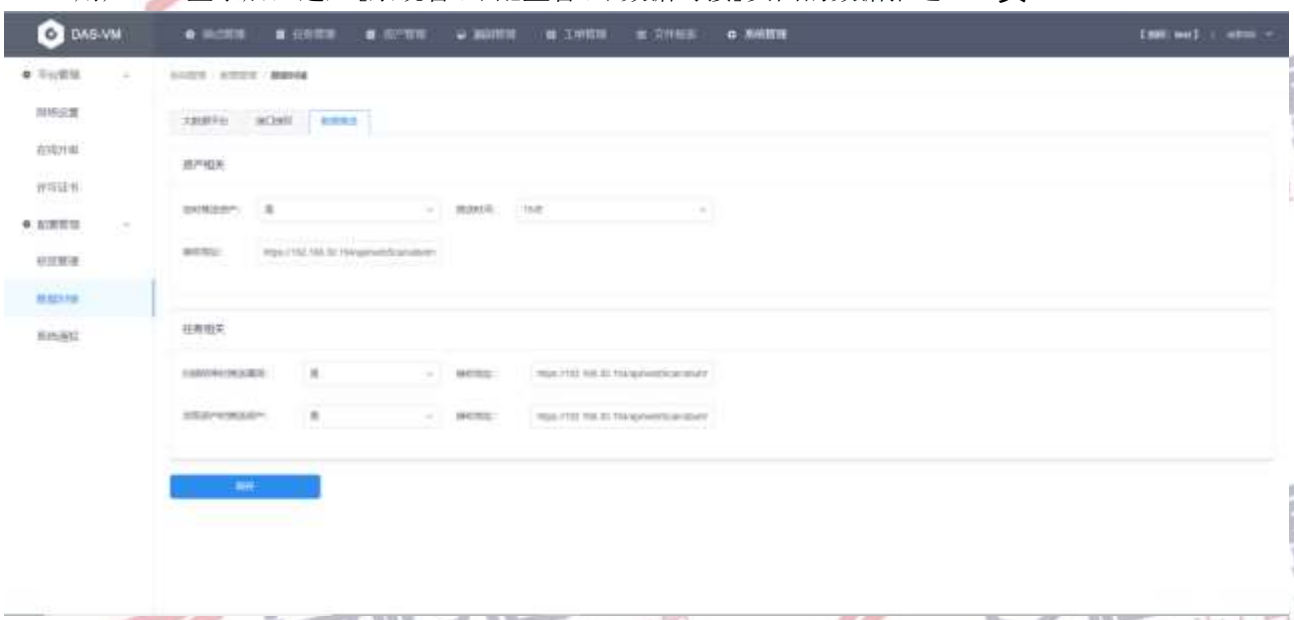
（2） 进入接口授权界面后，点击开启授权访问后，可以填写授权配置参数，点击<保存>按钮保存配置。

接口授权配置项及说明见下表：

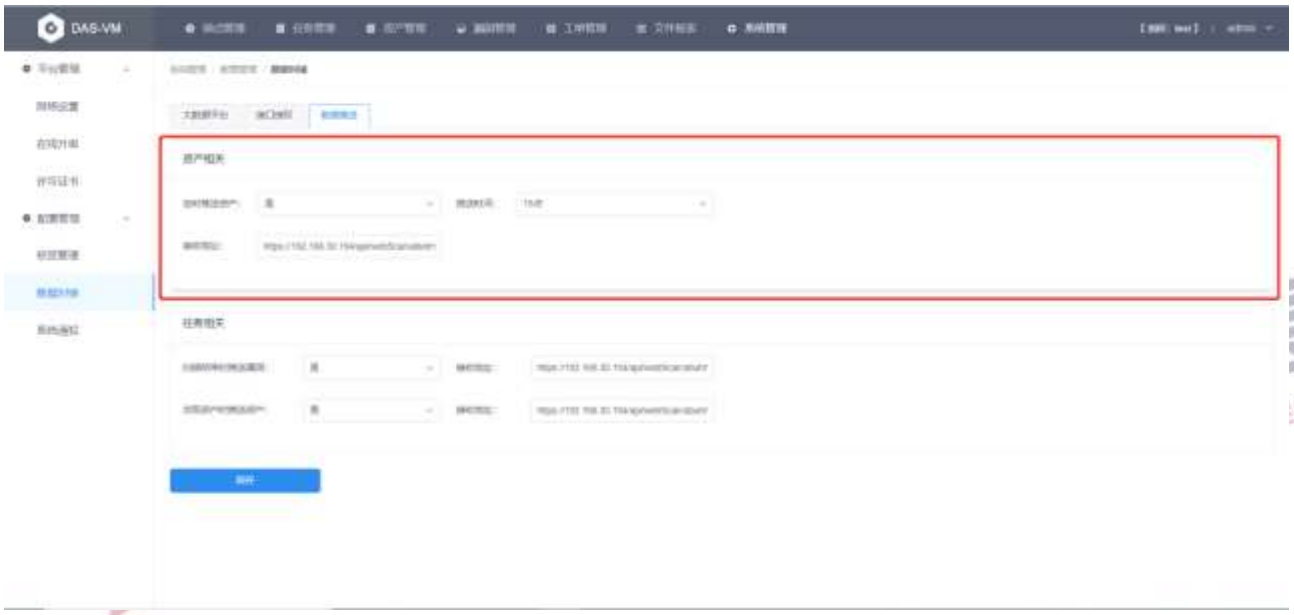
配置项	说明
允许访问的 IP	选择是否开启邮件通知
APIKey	必填项。设置邮件发信人

9.2.2.3. 数据推送

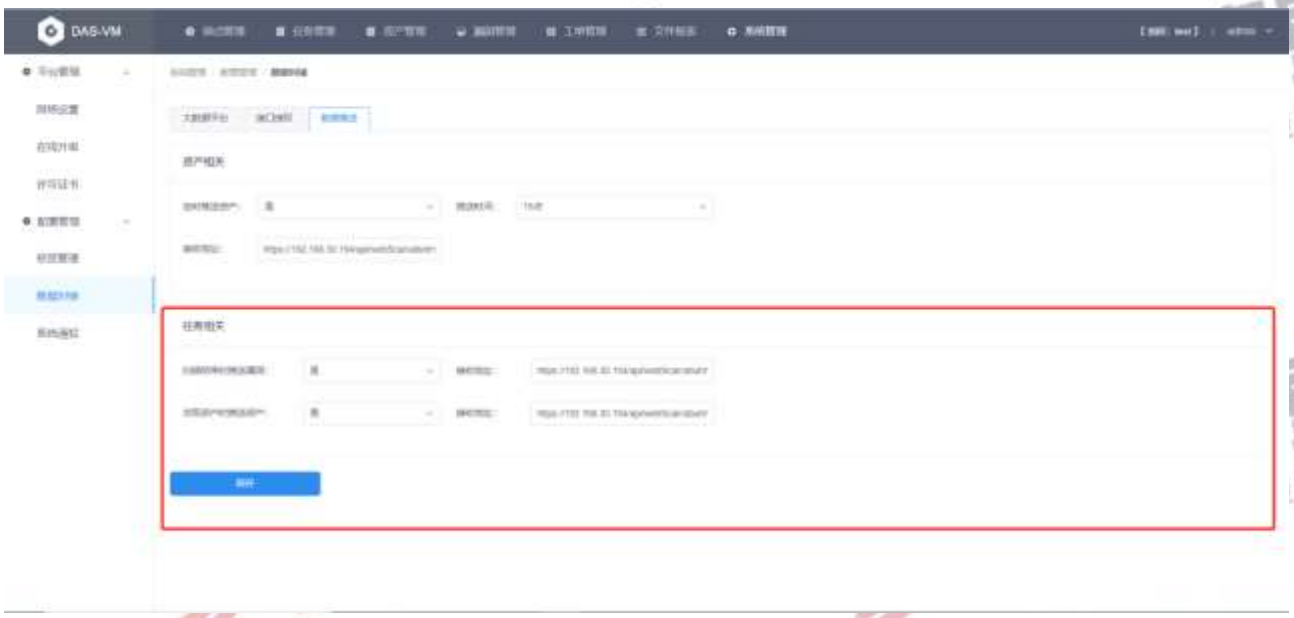
（1）用户 WEB 登录后，进入[系统管理/配置管理/数据对接]页面的数据推送 tab 页。



（2）数据推送界面中的资产相关部分中，可以选择是否定时推送资产，以及推送时间和接受地址。



（3）数据推送界面中的任务相关部分中，可以选择是否在扫描结束时推送漏洞和是否发现资产时推送资产，以及相关接收地址地址，自定义后点击<保存>按钮即可保存设置。



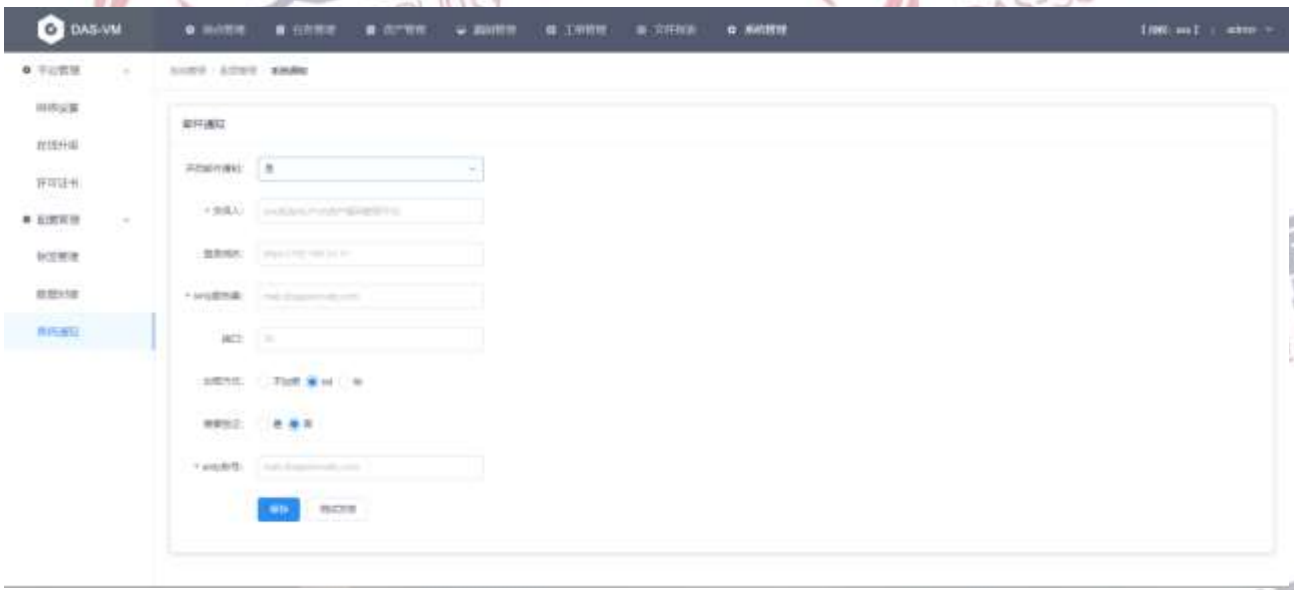
9.2.3. 系统通知

通知管理主要用于工单每步流转时向相应责任人发送邮件通知。

9.2.3.1. 邮件通知

（1） 用户 WEB 登录后，进入[系统管理/配置管理/系统通知]页面。

（2）开启邮件通知栏选择是，填写相关邮件通知配置信息，点击<保存>按钮，保存邮件邮件配置信息。

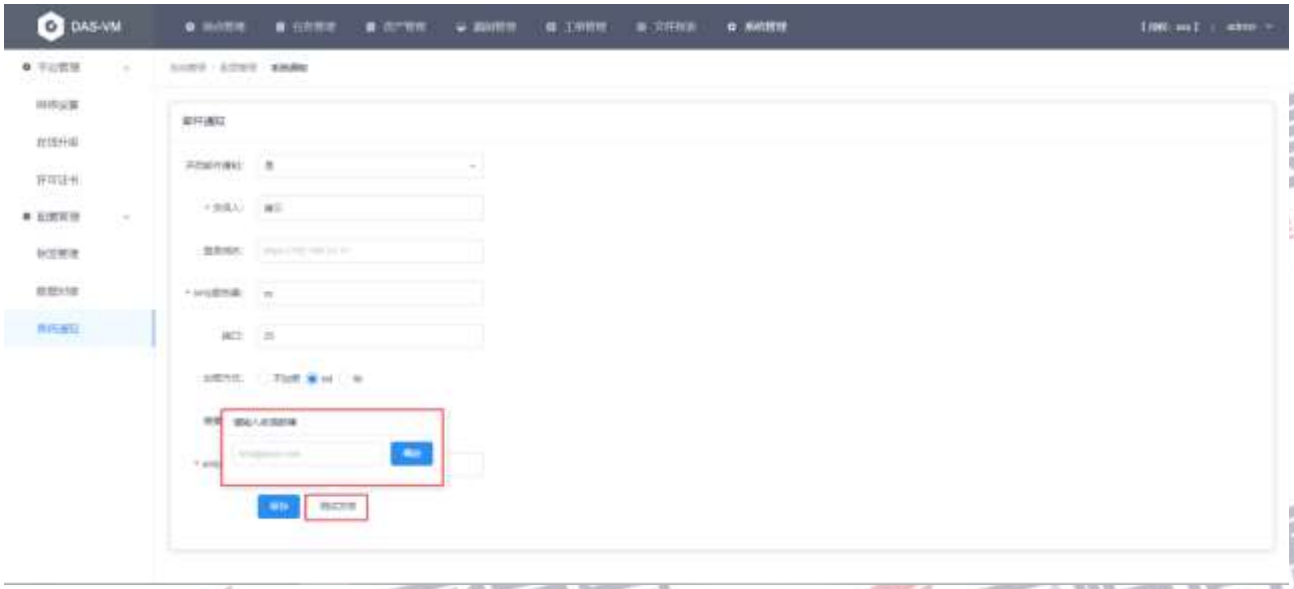


邮件通知配置项及说明见下表：

配置项	说明
开启邮件通知	选择是否开启邮件通知
发信人	必填项。设置邮件发信人
登录域名	选填项。设置平台的域名链接
smtp 服务器	必填项。设置邮件发送端服务器
端口	选填项。设置邮件发送端服务器的端口
加密方式	选择加密方式，包括不加密、ssl 和 tls
需要验证	选择是否需要密码验证
smtp 账号	必填项。设置邮件发送端服务器的登录账号

smtp 密码	必填项。当需要验证栏选择是时，设置邮件发送端服务器的登录密码

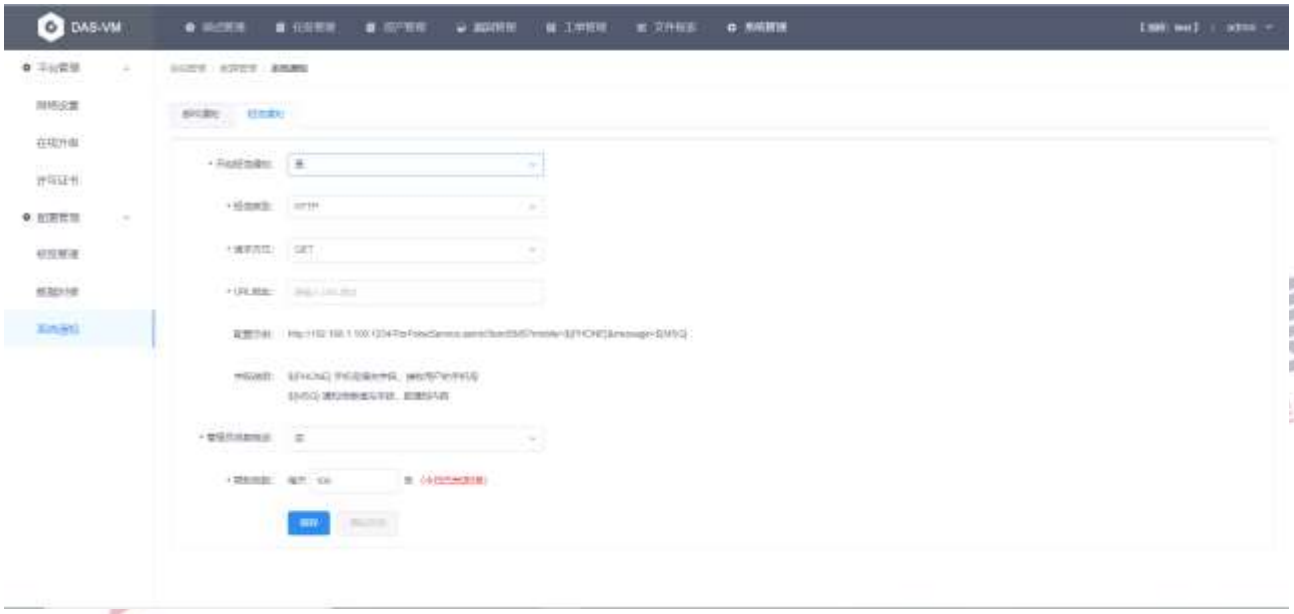
（3）完成邮件通知相关配置后，点击<测试发信>按钮，弹出收信邮箱输入框，输入收信邮箱，点击<确定>按钮，即可发送测试邮件至收信邮箱。



9.2.3.2. 短信通知

（1）用户 WEB 登录后，进入[系统管理/配置管理/系统通知]页面，点击<短信通知>。短信支持 Web Service 类型和 HTTP 类型的 GET 和 POST 两种请求方式。开启短信通知后，工单下发、流转的操作通知每隔五分钟（从整点开始算）向下一节点对象发送。工单撤回、提前结束、催办通知实时立即发送。支持短信每日发送条数上限设置。支持管理员消息推送开关设置。

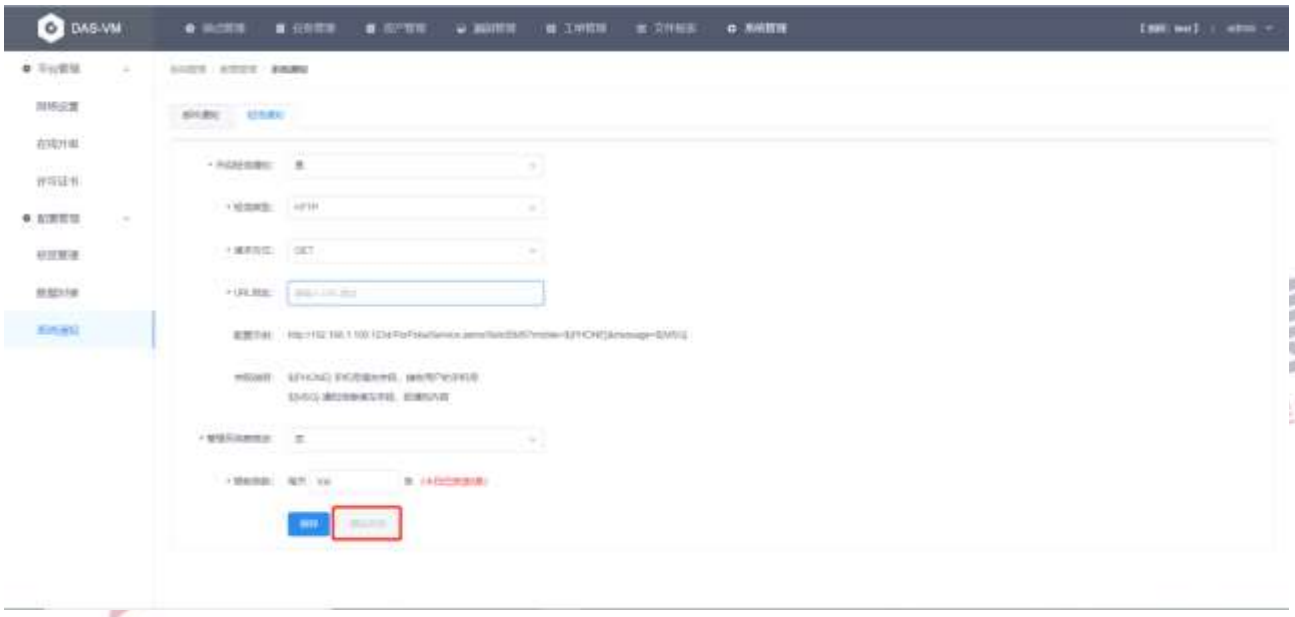
（2）开启短信通知栏选择是，填写相关通知配置信息，点击<保存>按钮，保存短信配置信息。



短信通知配置项及说明见下表：

配置项	说明
开启短信通知	选择是否开启短信通知
短信类型	必填项。
请求方式	选填项。
URL 地址	必填项。
管理员信息推送	必填项。选择是否接受管理员信息
限制条数	必填项。

（3）完成短信通知相关配置后，点击<测试发信>按钮，输入接收短信手机号码，点击<确定>按钮，即可发送测试短息至接收人。


DAS-VM

10. 用户管理

用户管理只有用户管理员才有此权限，其他用户不支持此功能，主要用于用户、角色的管理以及登录安全设置

10.1. 用户管理

用户管理主要用于用户、角色的管理

10.1.1. 用户列表

（1） 用户管理员 WEB 登录后，进入[系统管理/用户管理/用户列表]页面。用户列表默认用户包括 admin、useradmin 和 opadmin。

系统默认用户相关说明见下表：

用户	角色	用户名/密码	说明
admin	安全管理员	admin/r0x@z9lHw1c	安全管理员，权限包括：扫描引擎管理,查看报表,扫描分析,人工录入,已下发任务,扫描任务,误报列表,用户列表,扫描总览,自动发现,角色列表,资产总览。
opadmin	操作审计员	opadmin/Cw#190zHlRx	查看系统用户的操作日志
useradmin	用户管理员	useradmin/X9!Zcw01lhr	用户和角色的创建、删除等管理和登录安全设置

注意

系统自带的 3 个用户仅支持编辑操作且无法编辑角色，不支持删除操作。

10.1.1.1. 新增用户

（1） 点击<新增用户>按钮，弹出新增用户窗口，填写相应的信息，点击<保存>按钮，即可完成用户的添加。

用户信息各配置项及说明见下表：

配置项	说明
用户名	必填项。输入新增用户的名称，支持英文和中文名称
密码	必填项。输入新增用户的登录密码，建议 8~12 个字符，至少是数字和字母的组合
确认密码	必填项。输入新增用户的登录确认密码。确认是否和第一次的密码输入一致，不一致将无法创建成功
手机	选填项。输入新增用户的手机号码
邮箱	选填项。输入新增用户的邮箱地址
角色	必填项。选择用户所属角色

10.1.1.2. 编辑用户

（1） 点击用户列表中的<编辑>按钮，弹出编辑用户窗口，用户名无法编辑。

（2）单击<修改密码>按钮，进行密码修改，点击<取消密码>按钮，即可取消密码修改。

（3）编辑相应的配置项信息，单击<保存>按钮，即可完成用户信息的修改，单击<取消>按钮，取消用户信息修改。

注意

密码修改后，系统不做强制性退出，请单独退出重新登录。

10.1.1.3. 删除用户

（1） 点击用户列表中的<删除>按钮并确定，即可删除列表中相应的用户。

10.1.1.4. 解锁用户

当用户在规定时间内，多次连续登录失败，超过登录安全设置，用户会被锁定，而用户解锁功能，可对超出登录限制已锁定的用户进行解锁，解锁后用户可正常登录。

10.1.2. 角色列表

（1） 用户管理员 WEB 登录后，进入[系统管理/用户管理/角色列表]页面。角色列表默认角色包括安全管理员、操作审计员和用户管理员。

系统默认角色相关说明见下表：

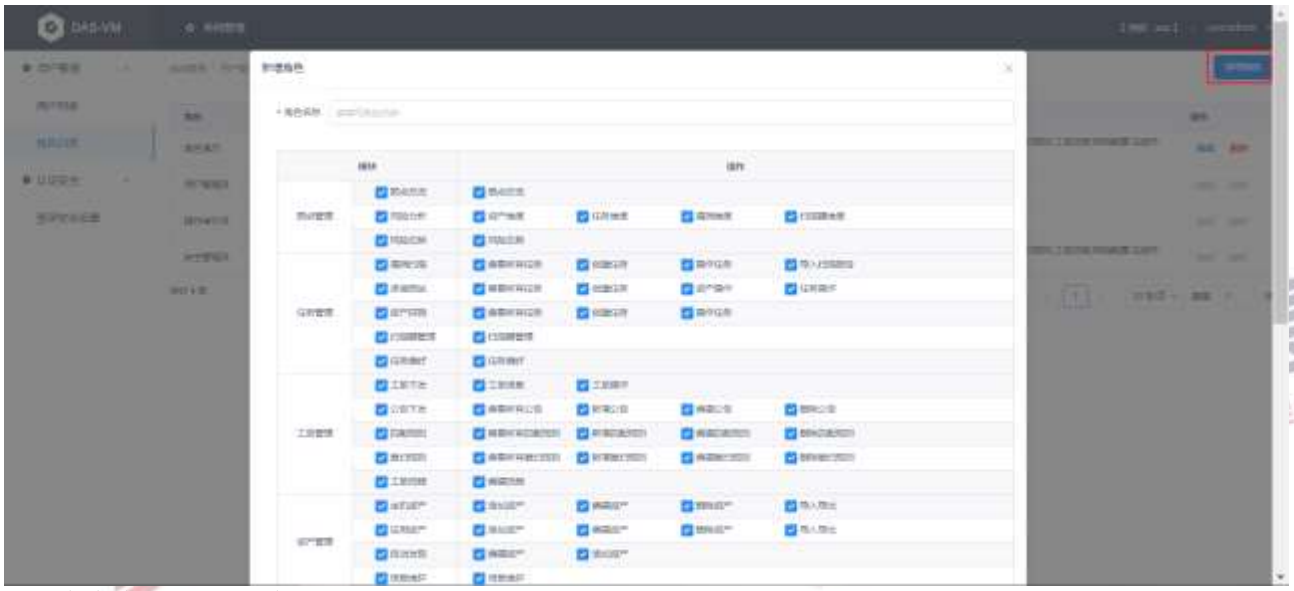
角色	权限说明
安全管理员	admin 用户登录的所有操作权限,包括弱点总览,漏洞扫描,渗透测试,风险分析,漏洞查询,误报库,已下发任务,公告下发,主机资产,应用资产,自动发现,报表统计,文件管理,下载管理,扫描引擎管理,网络配置,在线升级,偏好设置,标签管理,信息维护,许可证书,工单管理,数据推送,漏洞查询,资产探测
操作审计员	查看系统用户的操作日志
用户管理员	用户和角色的创建、删除等管理和登录安全设置

注意

系统自带的角色不能编辑、删除。

10.1.2.1. 新增角色

（1） 点击<新增角色>按钮，弹出新增角色窗口，填写相应的信息，点击<保存>按钮，即可完成角色的添加。



角色各配置项及说明见下表：

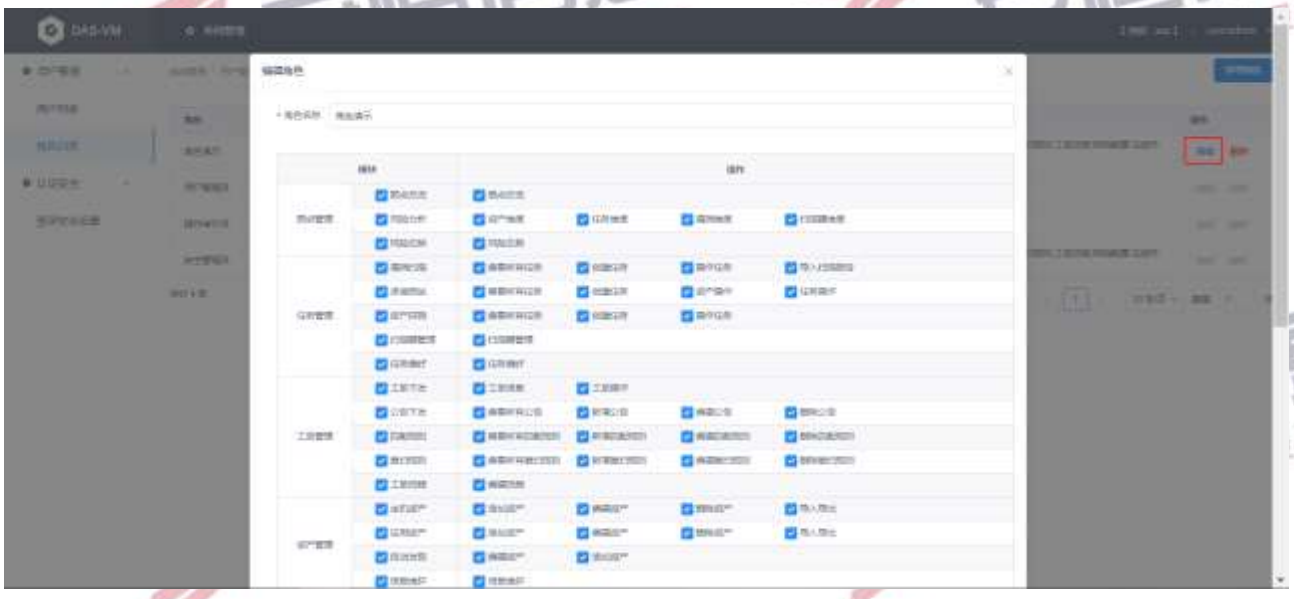
配置项	说明
角色名称	必填项。输入新增角色的名称
权限	可选项。选择新增角色具有的权限

说明

给用户分配权限时，只勾选了“模块”，而没有勾选模块下面的子功能的话，默认此用户只有查看分配此用户的任务和录入的漏洞详情，不能进行漏洞录入、提交结果等操作。

10.1.2.2. 编辑角色

（1） 点击角色列表中的<编辑>按钮，弹出编辑角色窗口，修改相应的角色名称以及勾选相应的权限，单击<保存>按钮，即可完成角色信息的修改。



10. 1. 2. 3. 删除角色

（1） 点击角色列表中的<删除>按钮并确定，即可删除列表中相应的角色。

10. 2. 登录安全

认证安全主要用于登录用户的一些安全设置，包括用户锁定、密码过期等信息配置

10. 2. 1. 登录安全设置

（1） 用户管理员 WEB 登录后，进入[系统管理/认证安全/登录安全设置]页面，可查看所有的登录安全配置信息。

登录安全设置各配置项及说明见下表：

配置项	说明
登录失败后锁定用户登录参数	用户可以自定义设置登入安全参数。如在 **60 秒**内，用户连续登录失败 5 **次**用户将被锁定 **5 分钟**。即该用户将在一分钟连续登录 5 次失败，将被锁定 5 分钟，5 分钟后将自动解锁。此设置防止不良攻击者进行暴力登录行为。可以对以上参数进行修改，修改后点击“保存”按钮即可
用户密码过期参数	可选择“启用”和“禁用”，可设置密码过期时间
用户登录超时时间	可设置用户登录系统后不做任何操作的超时时间
口令长度	可设置密码长度位数
口令复杂度	通过勾选来选择密码复杂度，包括：至少一个小写字母、至少一个大写字母、至少一个数字、至少一个特殊字符，口令必须包含至少两种字符的组合。

显示用户登录出错的详细信息	勾选后，登录时将提示出错的详细信息，如：用户登录可尝试次数，用户被锁定时间 反之就不提示详细信息
用户登录出错，记录日志	勾选后，用户登录失败日志将记录系统日志 反之就不记录
用户登录是否需要验证码	勾选后，用户登录时需要输入对应的验证码 反之就不需要

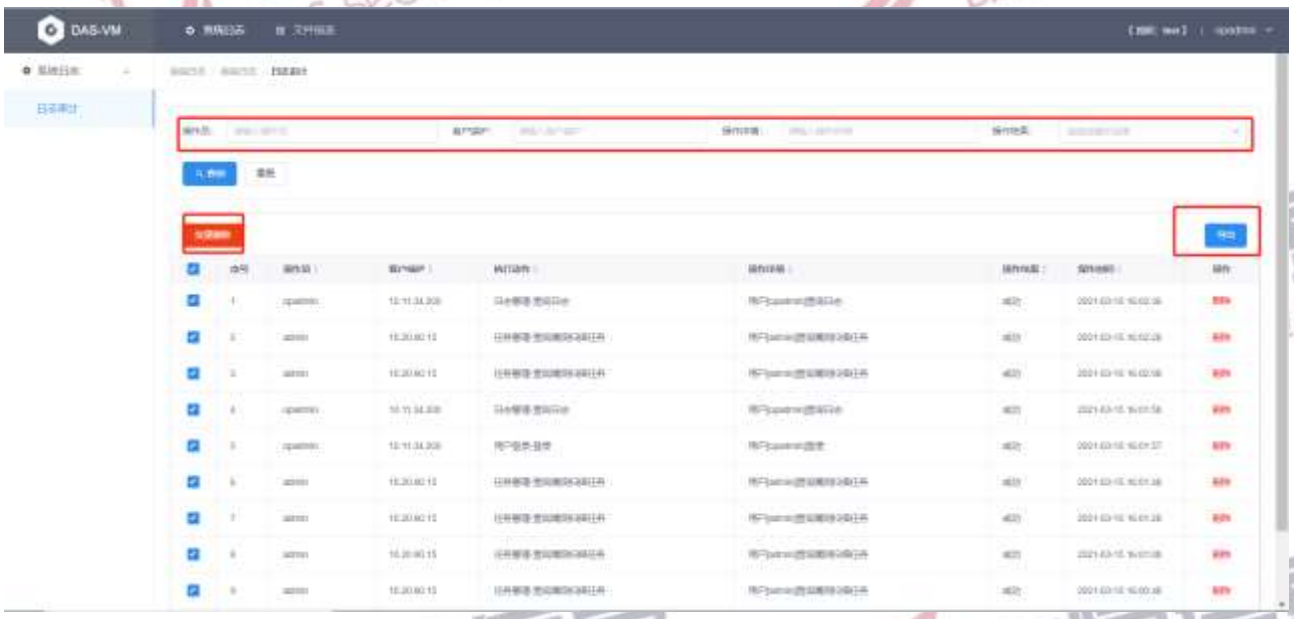
11. 系统日志

记录系统相关的日志信息。系统日志记录了用户通过平台对系统进行的操作行为。

> 说明
>
> 系统日志只有操作审计员才能进行查看。
>
> 操作审计员的初始用户名为 opadmin，初始密码为 Cw#190zHlRx。

11.1. 日志审计

（1） 在登录页面，用户名输入：opadmin，密码：Cw#190zHlRx，登录系统，默认展示日志审计页面，实时展示系统日志记录信息，包括操作员、客户端 IP、执行动作、详细信息、操作结果、操作时间。支持操作日志查询、排序、导出、删除功能，日志审计员用户可对操作日志进行查询、排序、导出、删除等操作。支持导出指定查询条件下的日志，导出格式为 excel。支持批量删除。



11.2. 文件报表

（1）在文件报表下，显示日志审计界面选择导出的的文件，导出后可进行下载和删除。

12. 工单系统

工单系统主要用于责任人进行工单处理的管理

12.1. 页面登录

（1） 在浏览器中输入 *https://管理 IP*，进入登录窗口，在登录窗口中点击<切换到工单系统>按钮，切换到工单系统登录窗口。

（2） 切换到工单系统登录窗口后输入用户名、密码，点击<登录>按钮后，进入[工单信息/安全运营/工作台]页面。

说明

浏览器目前支持 Chrome、火狐。

工单系统的用户名和密码说明：

用户名：责任人手机号（可在弱点管理平台中的[资产管理/资产相关/信息维护/人员维护]页面中查看责任人的手机号）。

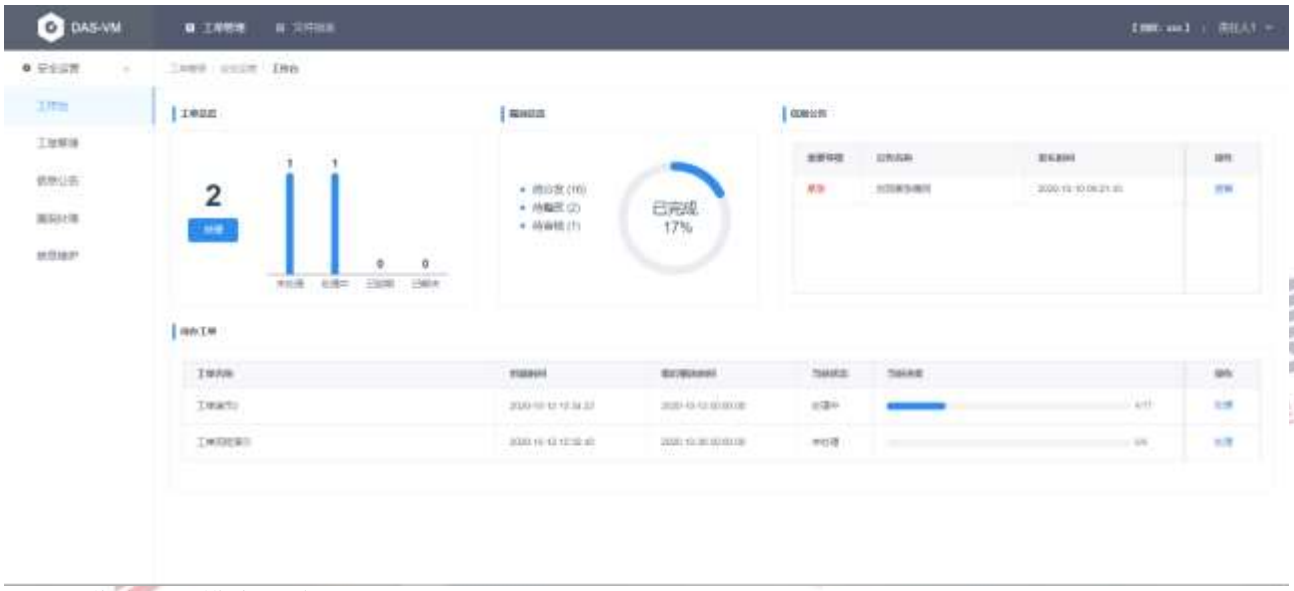
密码默认为：hL9r@X1cOWz。

12.2. 工单管理

12.2.1. 工作台

工作台主要展示工单的总体信息，包括工单总览、漏洞总览、信息公告和待办工单。

（1） 责任人用户 WEB 登录后，进入工单系统[工单管理/安全运营/工作台]页面。



工作台相关模块及说明见下表：

模块	说明
工单总览	展示当前登录用户的工单处理情况。
漏洞总览	展示当前登录用户未完成工单的漏洞处理情况。
信息公告	展示最新的三条公告信息。
待办工单	展示当前登录用户最新的五条未完成工单。

12.2.1.1. 工单总览

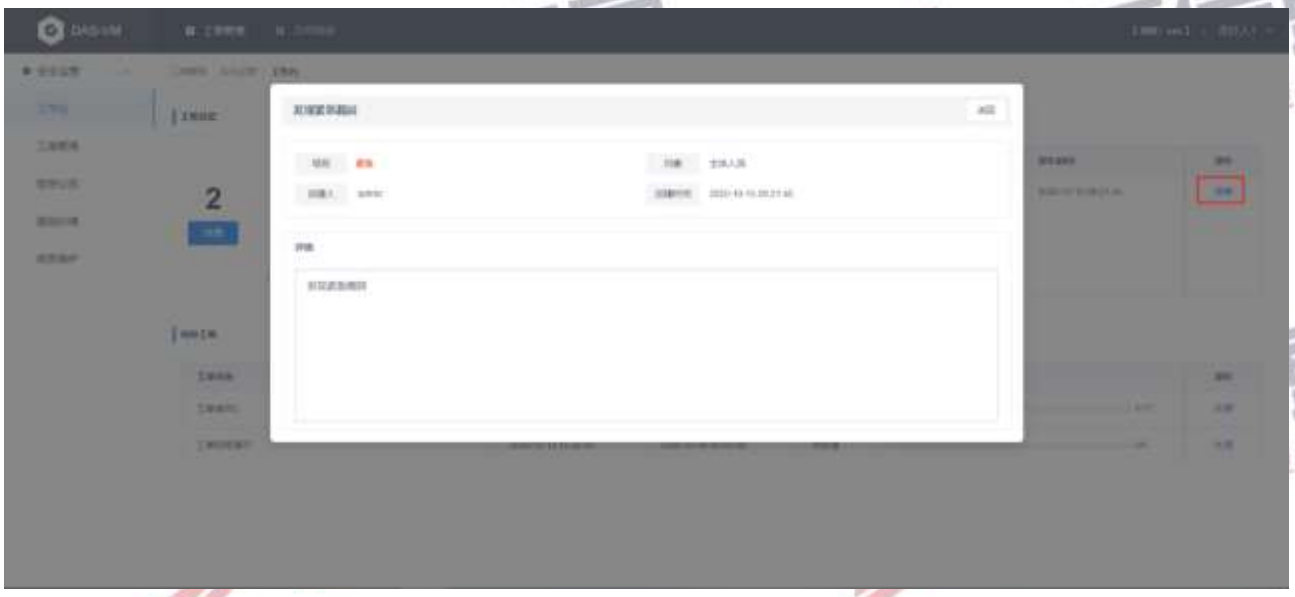
（1）工单总览栏展示当前登录用户的工单处理情况，统计未处理、处理中、已延期、已解决的工单个数及未完成工单个数。点击<处理>按钮可快速跳转至[工单管理/安全运营/工单管理]页面查看具体的工单列表。

12.2.1.2. 漏洞总览

（1） 漏洞总览栏展示当前登录用户未完成工单的漏洞处理情况，统计待分发、待整改和待审核的漏洞个数个数及漏洞处理完成度。

12.2.1.3. 信息公告

（1） 信息公告栏展示最新的三条公告信息，点击<查看>按钮可查看相应公告的具体信息。



12.2.1.4. 待办工单

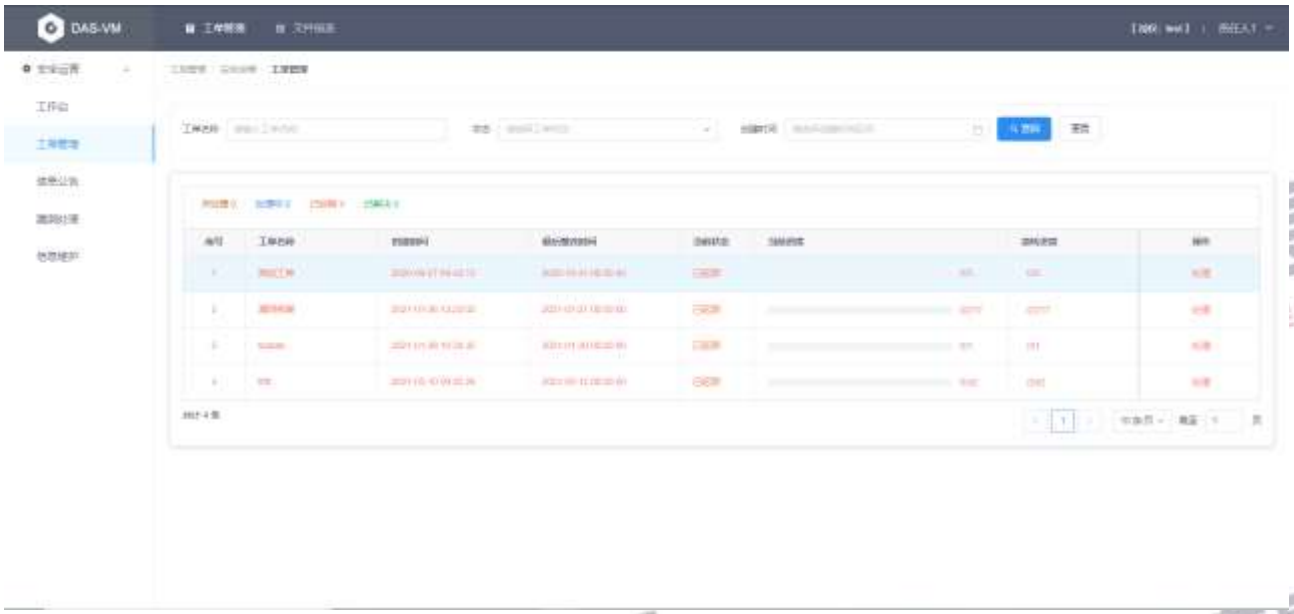
（1） 待办工单栏展示当前登录用户最新的五条未完成工单。点击待办工单列表的<处理>按钮可快速跳转至[工单管理/安全运营/漏洞管理]页面快速处理该工单的漏洞。

12.2.2. 工单管理

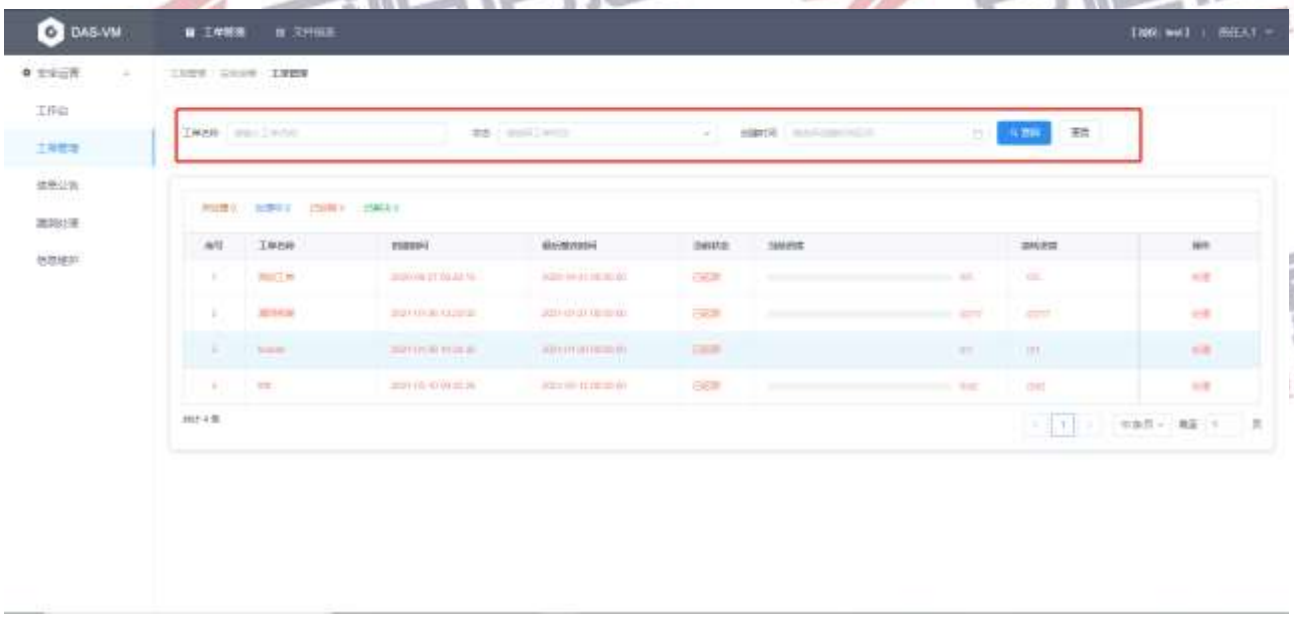
工单管理主要用于管理工单。

12.2.2.1. 工单查询

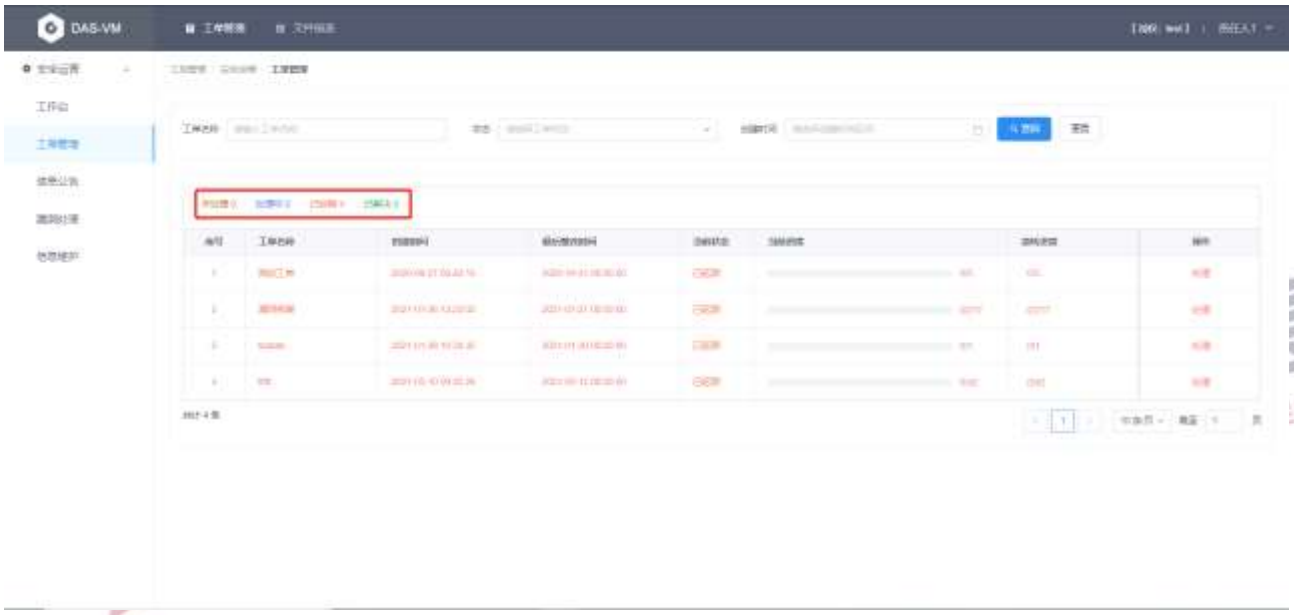
（1） 责任人用户 WEB 登录后，进入工单系统[工单管理/安全运营/工单管理]页面。



（2） 设置查询条件，可在工单管理列表中进行指定工单查询，条件设置后，点击<查询>按钮，进行查询。点击<重置>按钮，可清空查询条件。

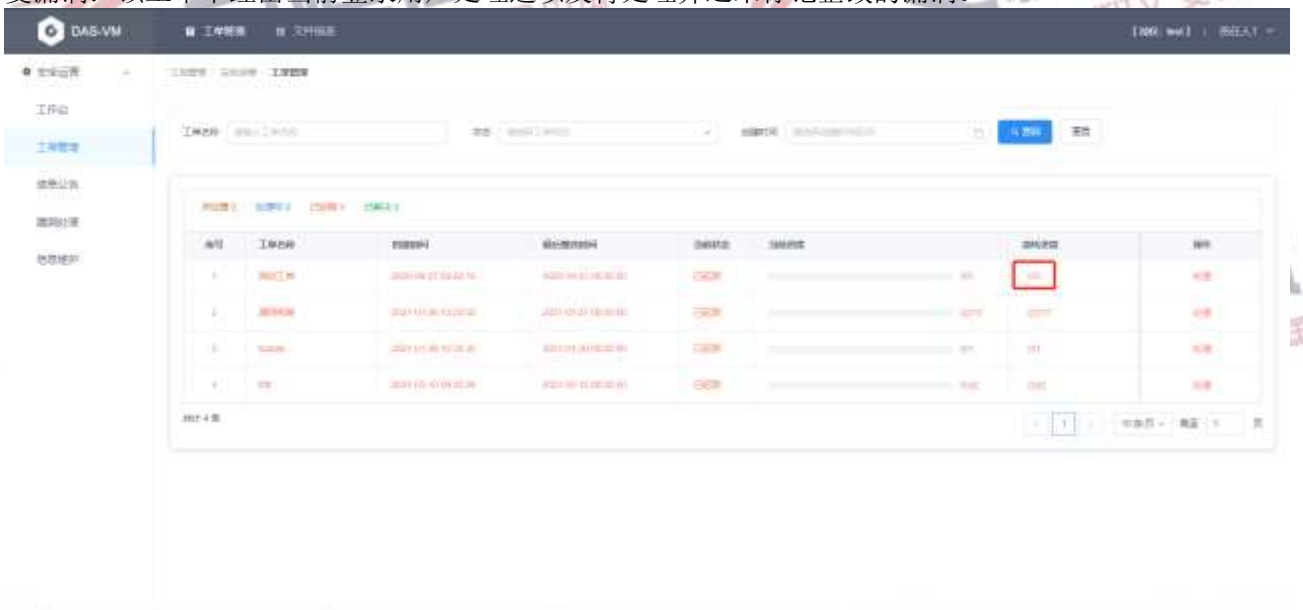


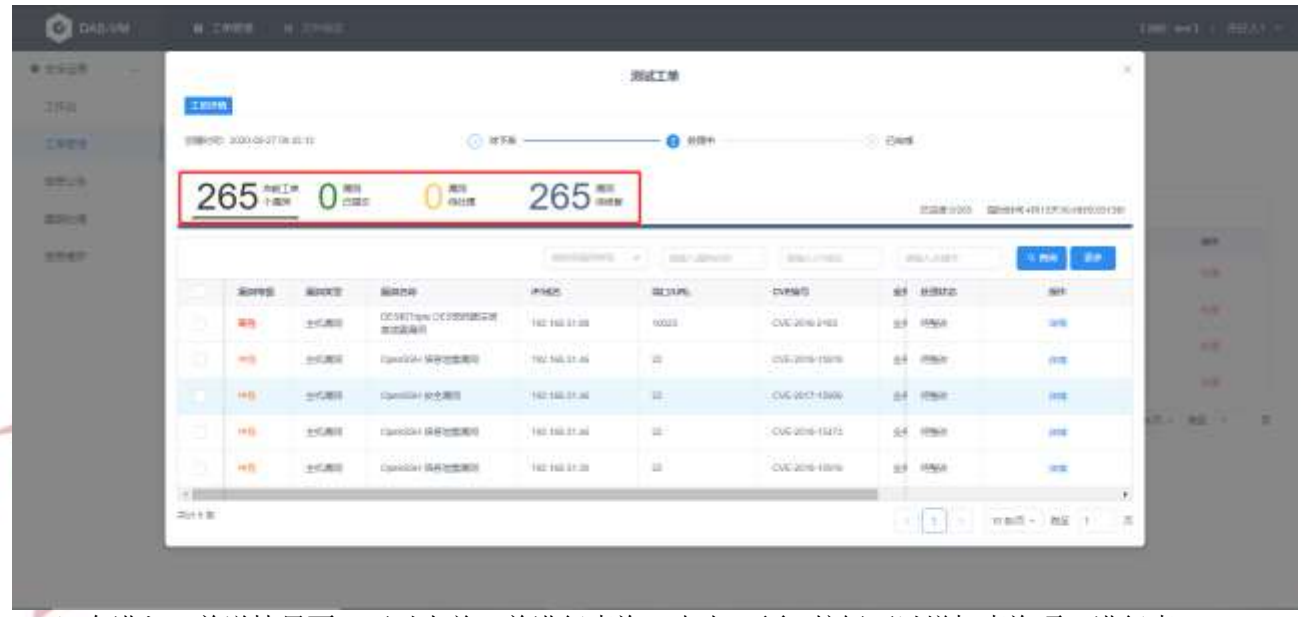
（3） 点击工单状态，可切换查看不同处理状态的工单列表。



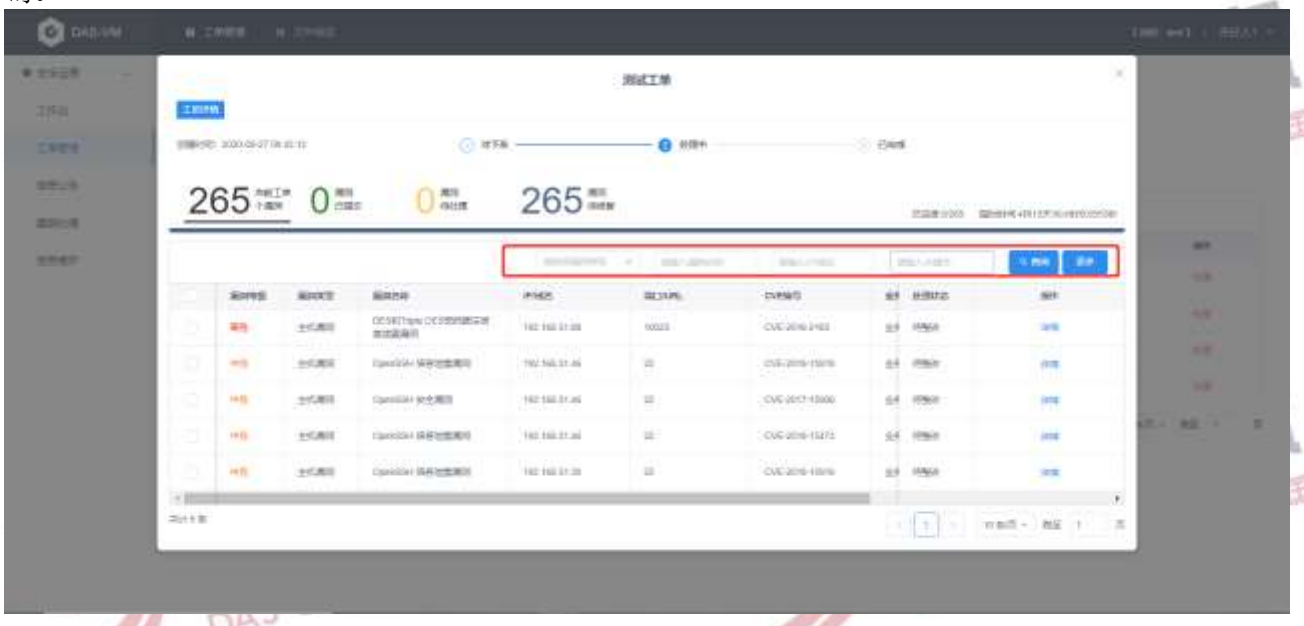
12.2.2.2. 工单流转进度

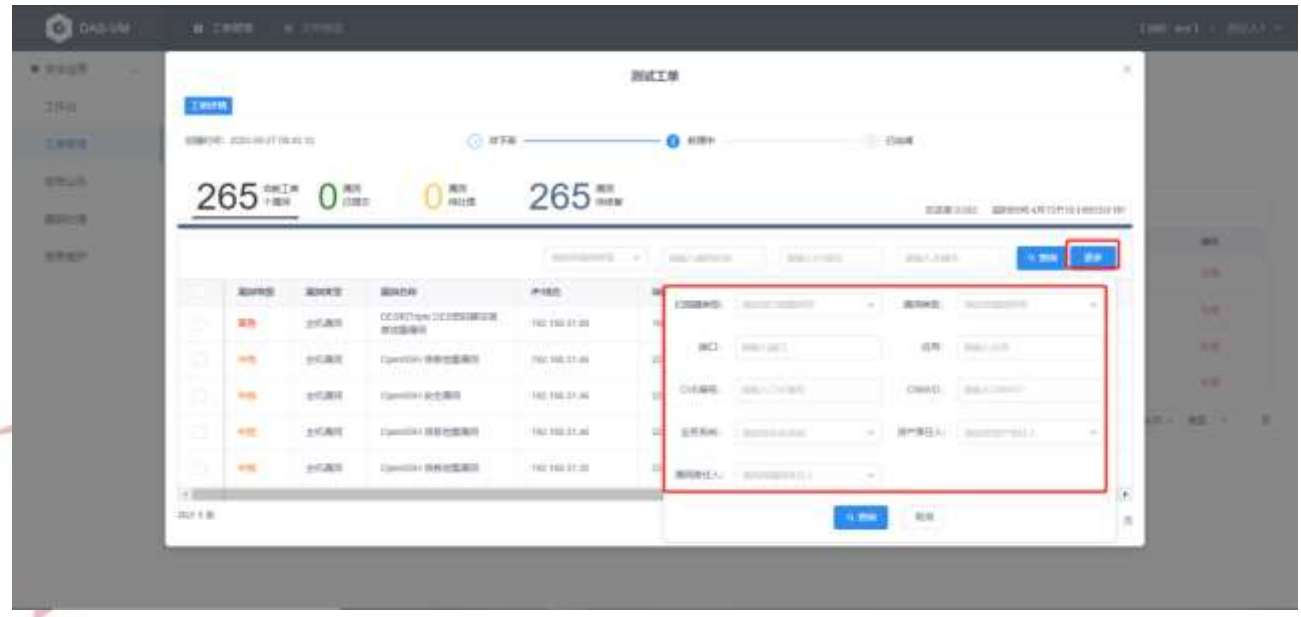
（1）工单用户点击流转进度可查看该工单经由当前登录用户处理过流转出去的和待处理的漏洞列表，当前工单漏洞：当前工单内所有经由当前登录用户处理过和待处理漏洞；
已提交漏洞：该工单中经由当前登录用户处理过并提交至管理平台的漏洞；
待处理漏洞：待当前登录用户处理的漏洞；
待修复漏洞：该工单中经由当前登录用户处理过以及待处理并还未标记整改的漏洞。





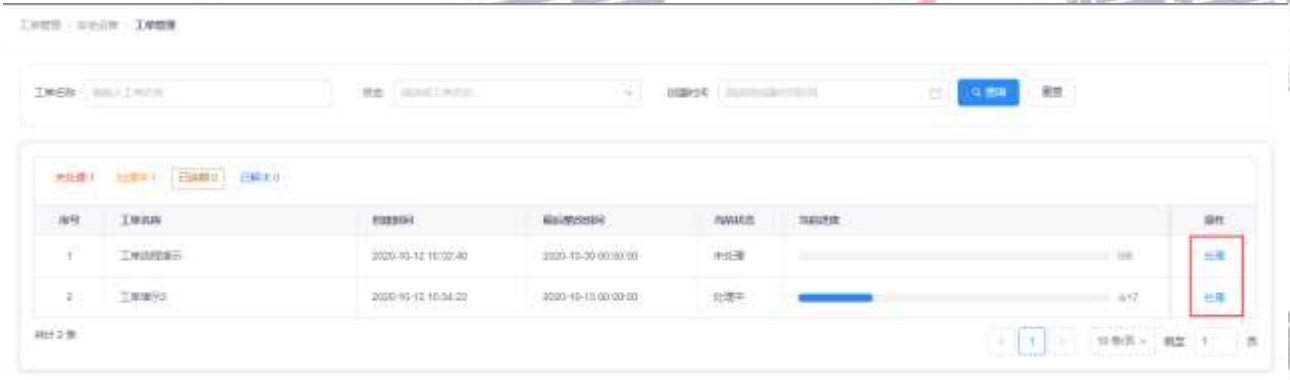
（2）在进入工单详情界面，可对当前工单进行查询，点击<更多>按钮可以增加查询项，进行查询。





12.2.2.3. 工单处理

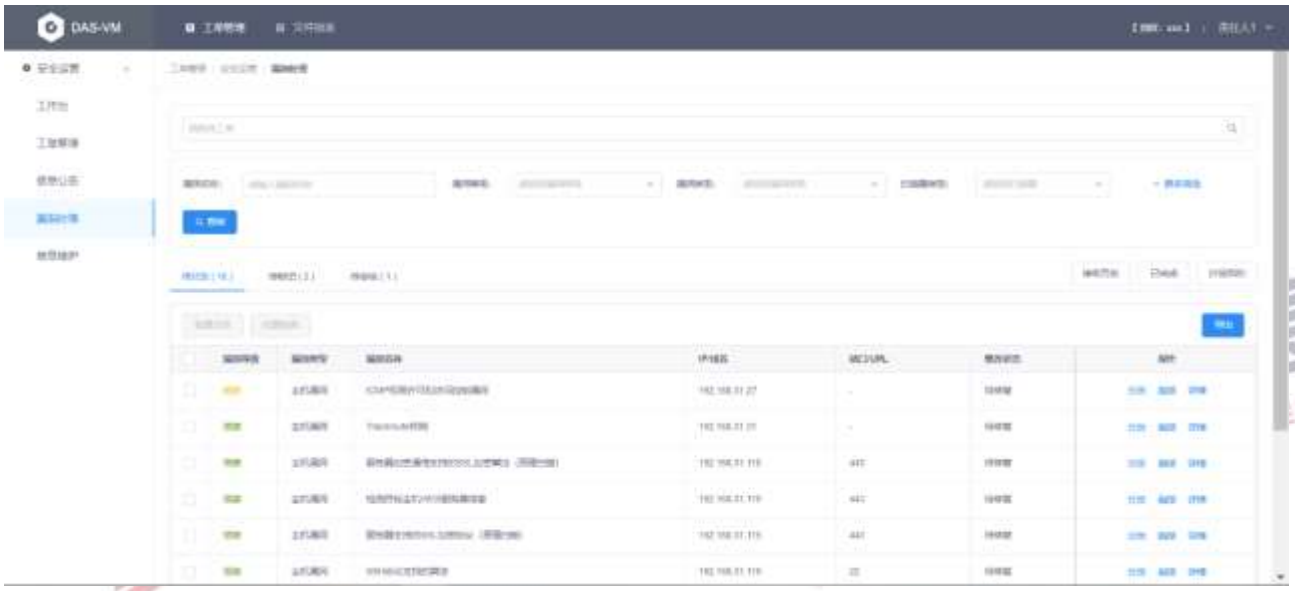
（1） 点击工单列表的<处理>按钮，可快速跳转至[工单管理/安全运营/漏洞管理]页面快速处理该工单的漏洞。



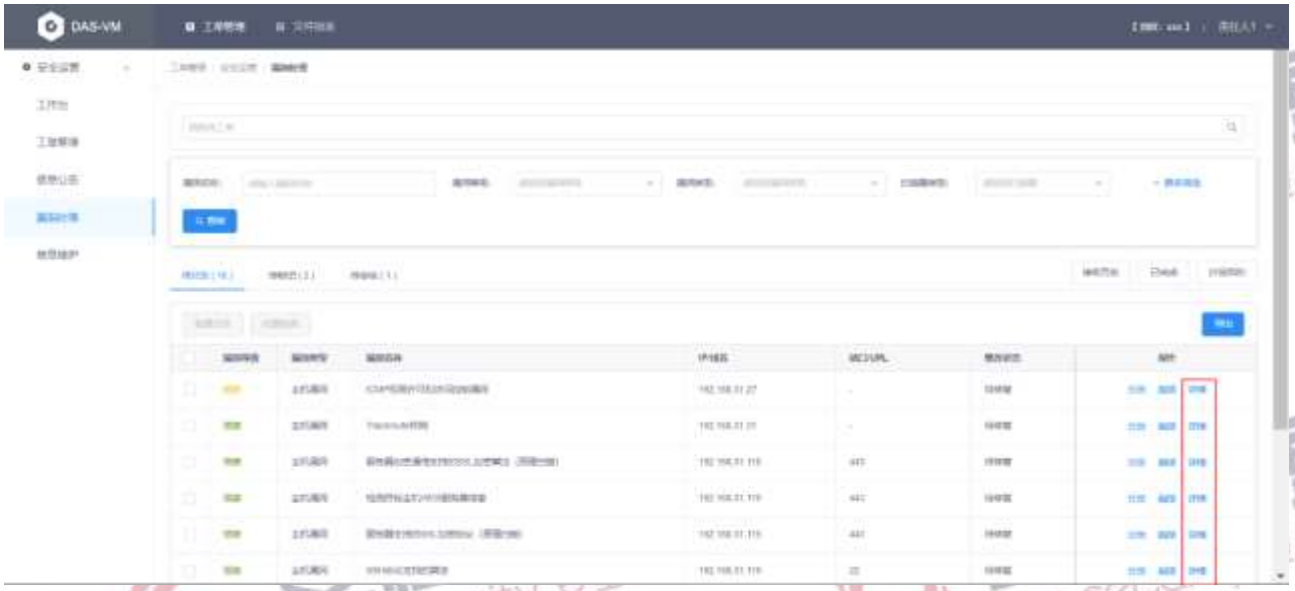
12.2.3 漏洞处理

12.2.3.1. 漏洞详情

（1） 拥有分发漏洞权限的责任人用户 WEB 登录后，进入工单系统[工单管理/安全运营/漏洞处理]页面。

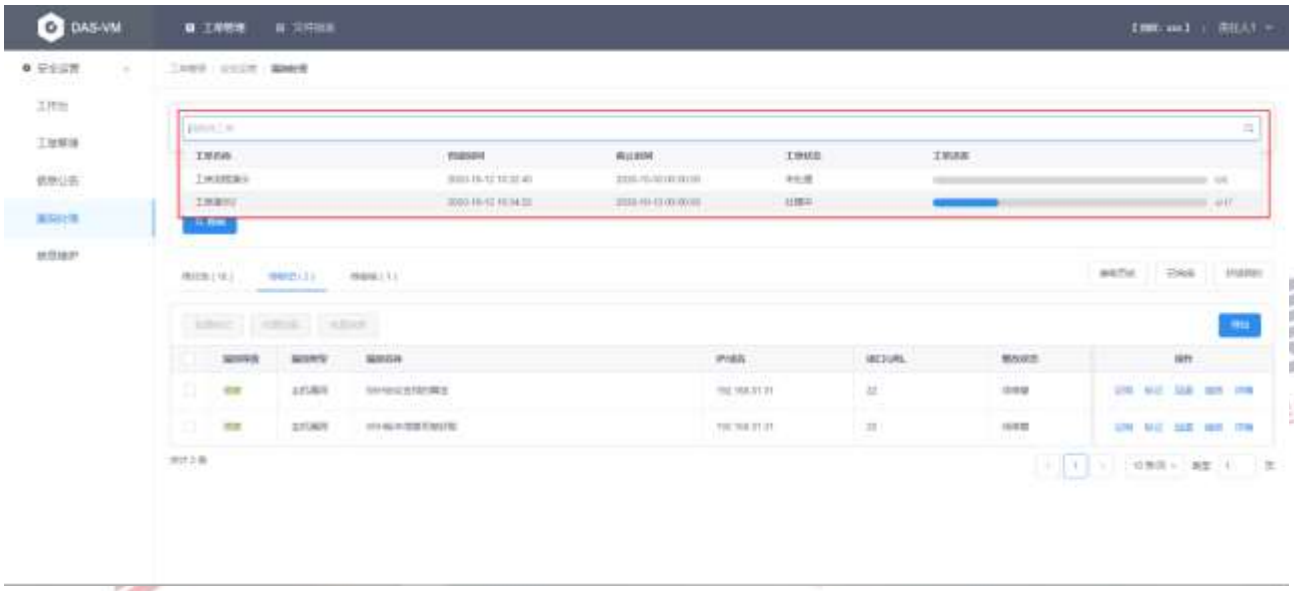


（2） 在漏洞列表点击<详情>按钮可查看漏洞的漏洞详情。



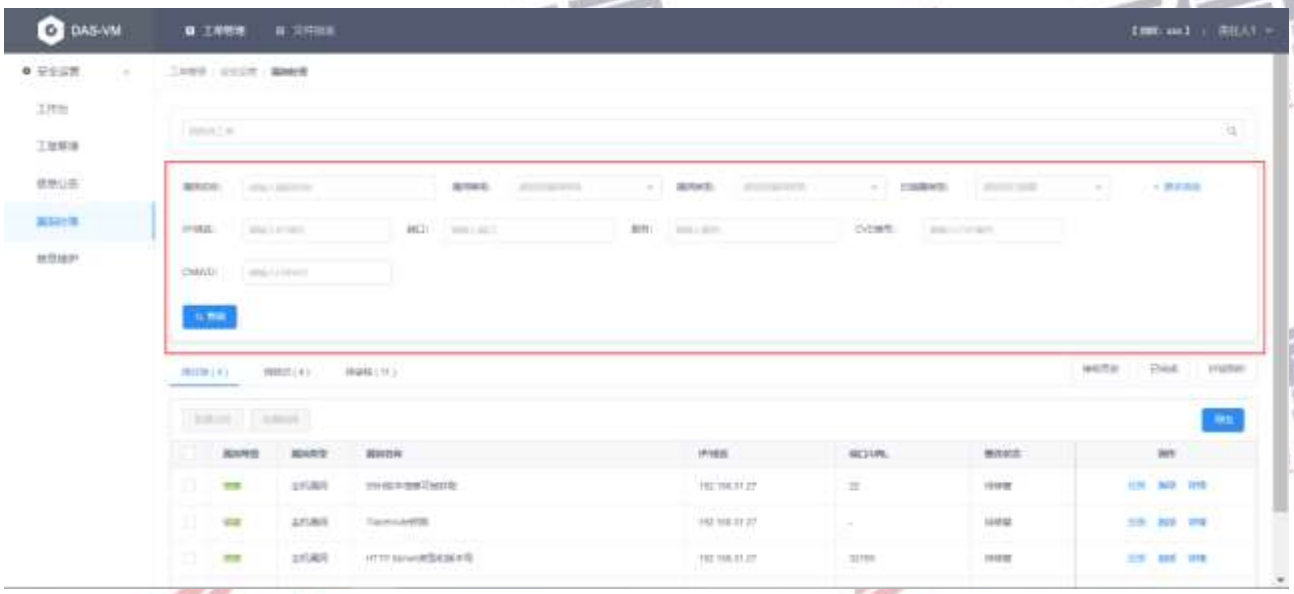
12.2.3.2. 选择工单

（1） 点击<请选择工单>下拉展示未完成工单列表，选择工单，进入该工单漏洞处理页面。



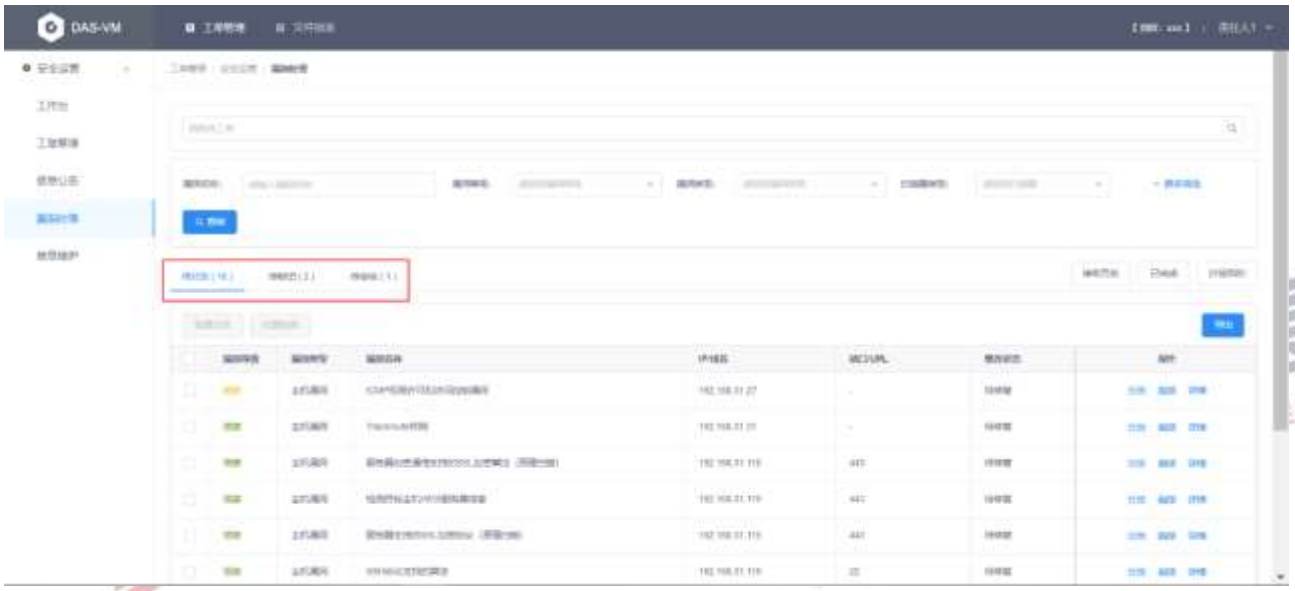
12.2.3.3. 查询漏洞

（2）设置查询条件，可在漏洞处理页面漏洞列表中进行指定漏洞查询，点击<更多筛选>按钮，可以下拉展示更多查询条件；条件设置后，点击<查询>按钮，进行查询。

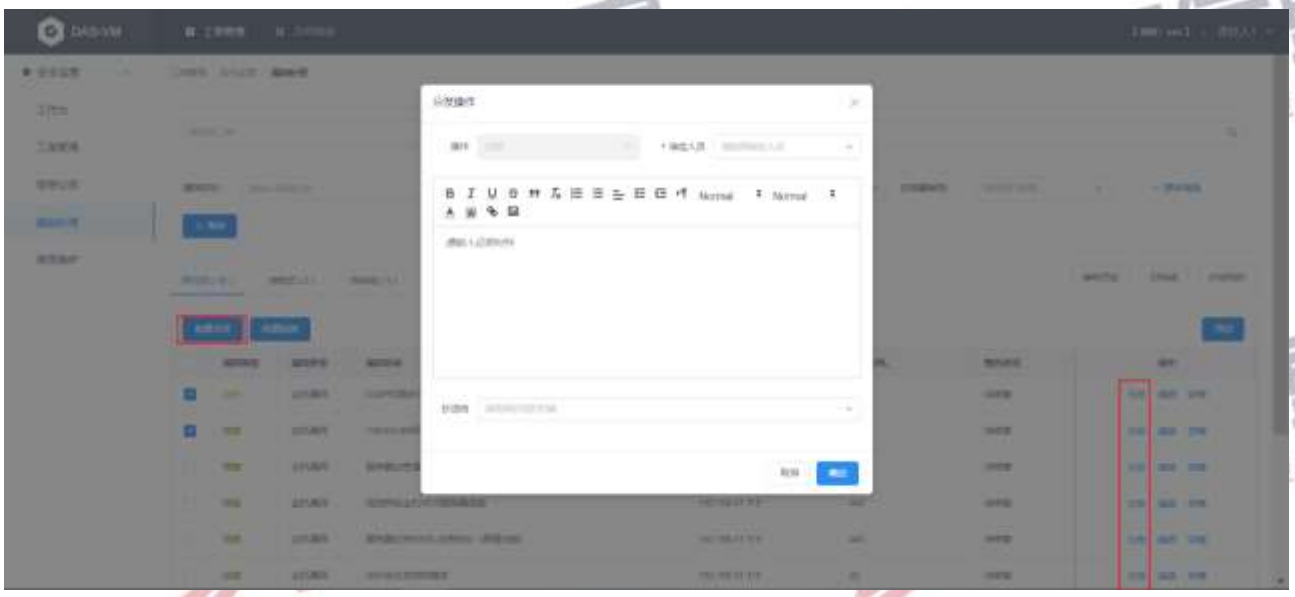


12.2.3.4. 分发漏洞

（1）拥有分发漏洞权限的责任人用户 WEB 登录后，进入工单系统[工单管理/安全运营/漏洞处理]页面，漏洞状态栏点击<待分发>查看待分发漏洞列表。

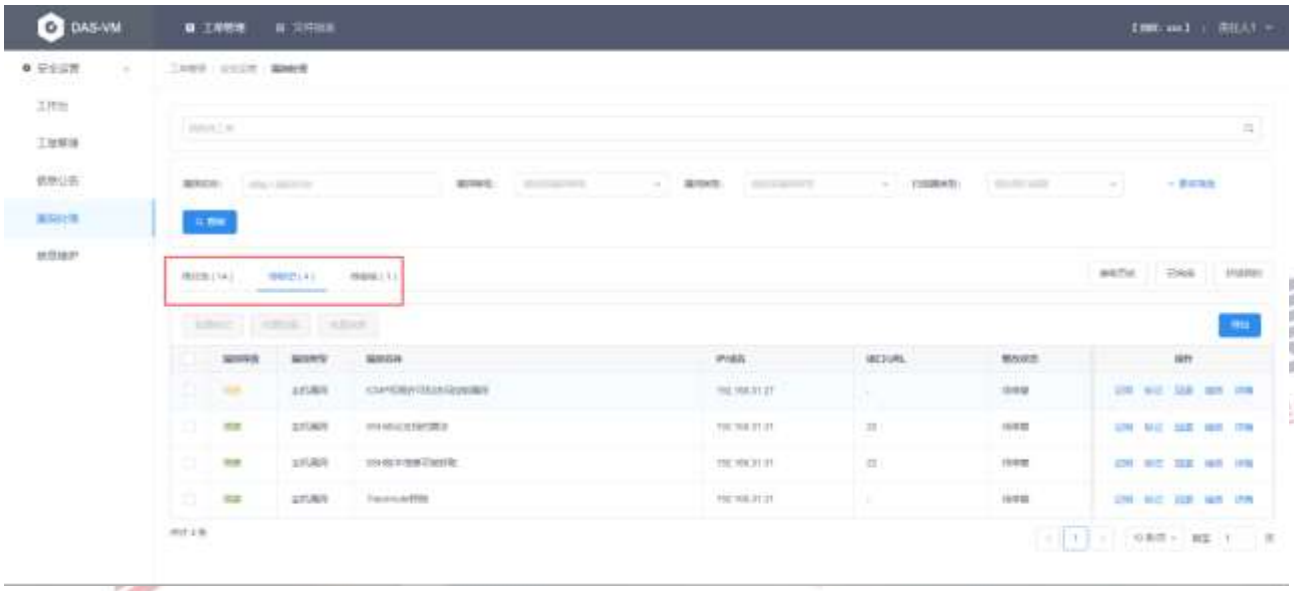


（2）待分发列表点击<分发>按钮或勾选多个漏洞点击<批量分发>按钮，指定下一节点的人员，填写证明材料，点击<确定>按钮即可将漏洞指分发给下一节点的人员。若需要抄送其他人在抄送对象栏选择抄送对象。

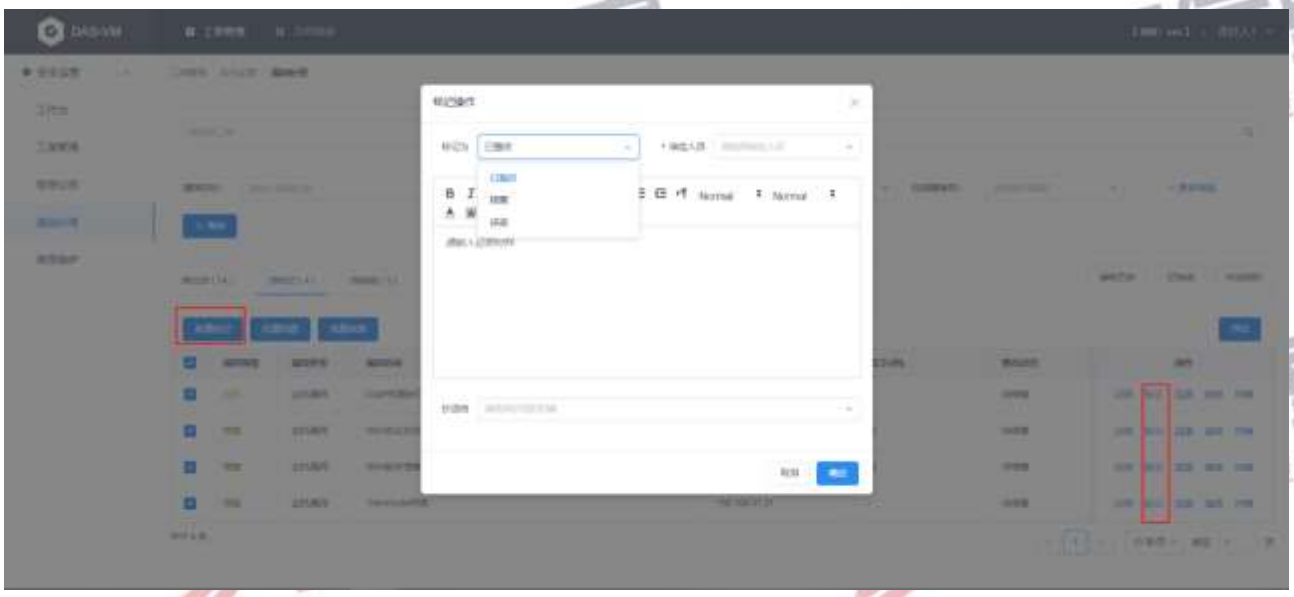


12.2.3.5. 标记漏洞

（1）拥有整改漏洞权限的责任人用户 WEB 登录后，进入工单系统[工单管理/安全运营/漏洞处理]页面，漏洞状态栏点击<待标记>查看待标记漏洞列表。

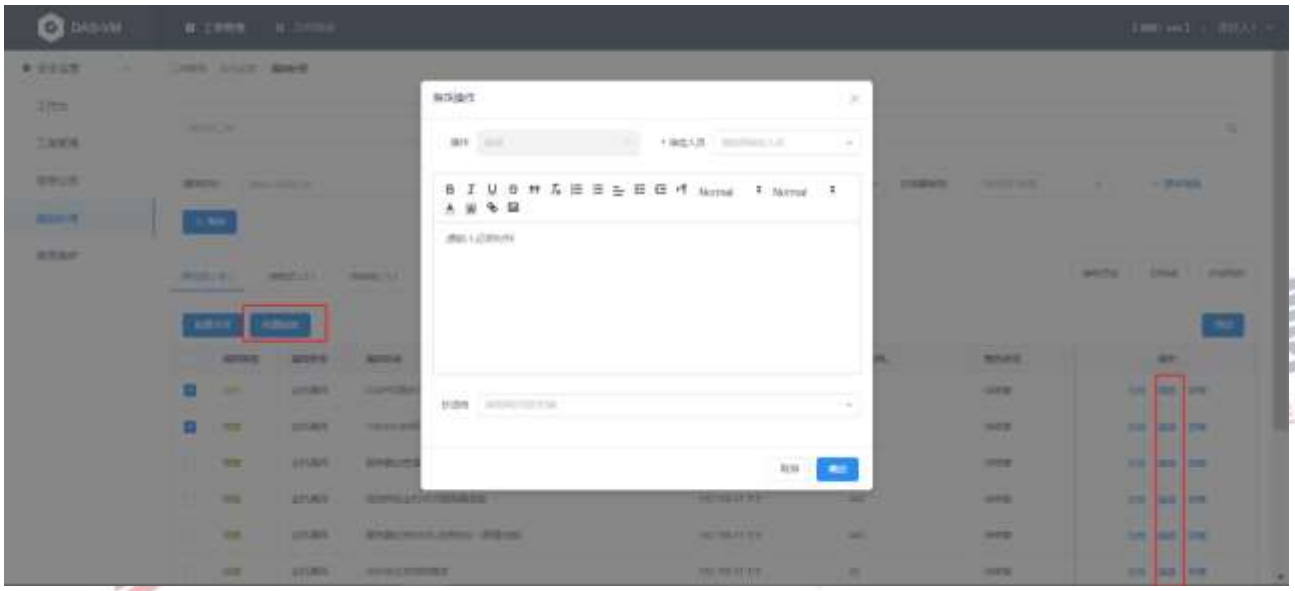


（2）待标记列表点击<标记>按钮或勾选多个漏洞点击<批量标记>按钮，选择标记状态，指定下一节点的人员，填写证明材料，点击<确定>按钮即可将漏洞提 交给下一节点的人员。若该节点下一节点为管理平台，则无需指定人员。若需要抄送其他人在抄送对象栏选择抄送对象。



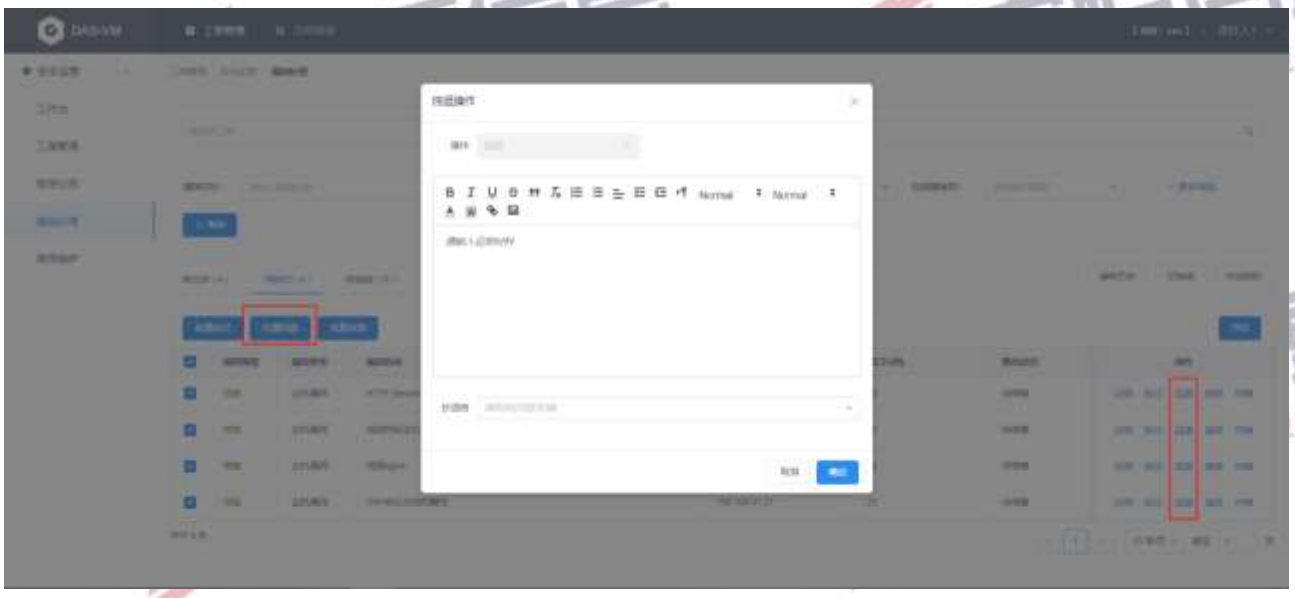
12.2.3.6. 指派漏洞

（1）若需要将漏洞转移给同节点的其他人员，可在待分发列表点击<指派>按钮或勾选多个漏洞点击<批量指派>按钮，指定同节点的其他人员，填写证明材料，点击<确定>按钮即可将漏洞指派给同节点的其他人员。若需要抄送其他人在抄送对象栏选择抄送对象。



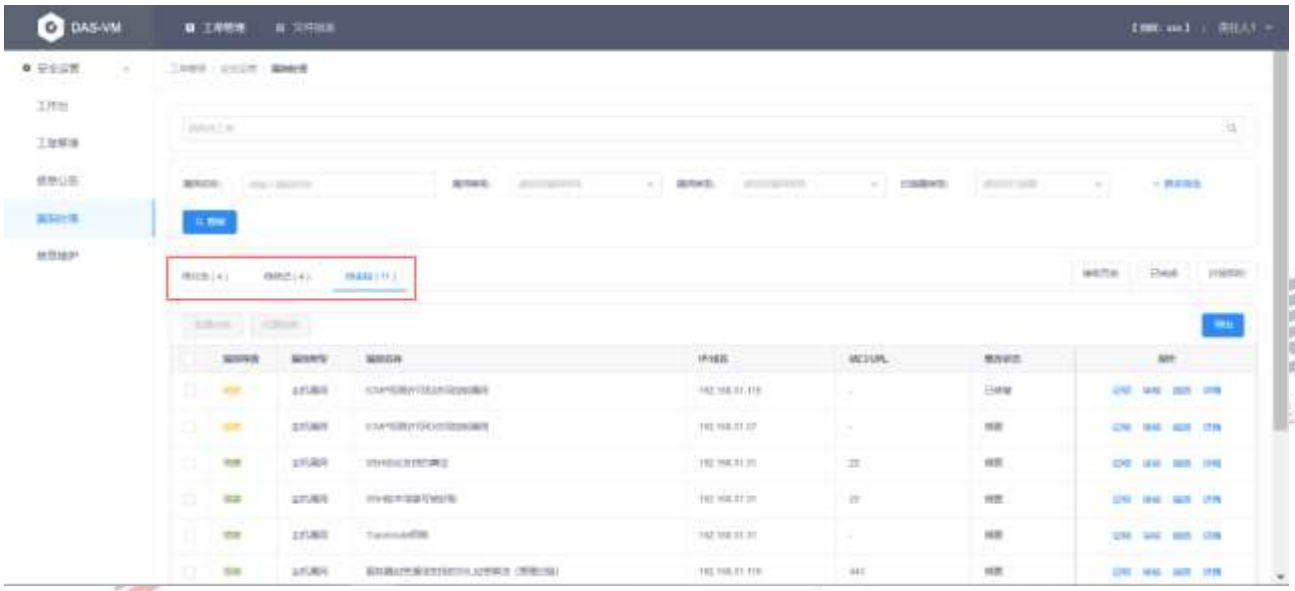
12.2.3.7. 回退漏洞

（1）若需要将漏洞回退给上一节点的人员，可在漏洞列表点击<回退>按钮或勾选多个漏洞点击<批量回退>按钮，填写证明材料，点击<确定>按钮即可将漏洞回退给上一节点提交漏洞的人员。若需要抄送其他人可在抄送对象栏选择抄送对象。

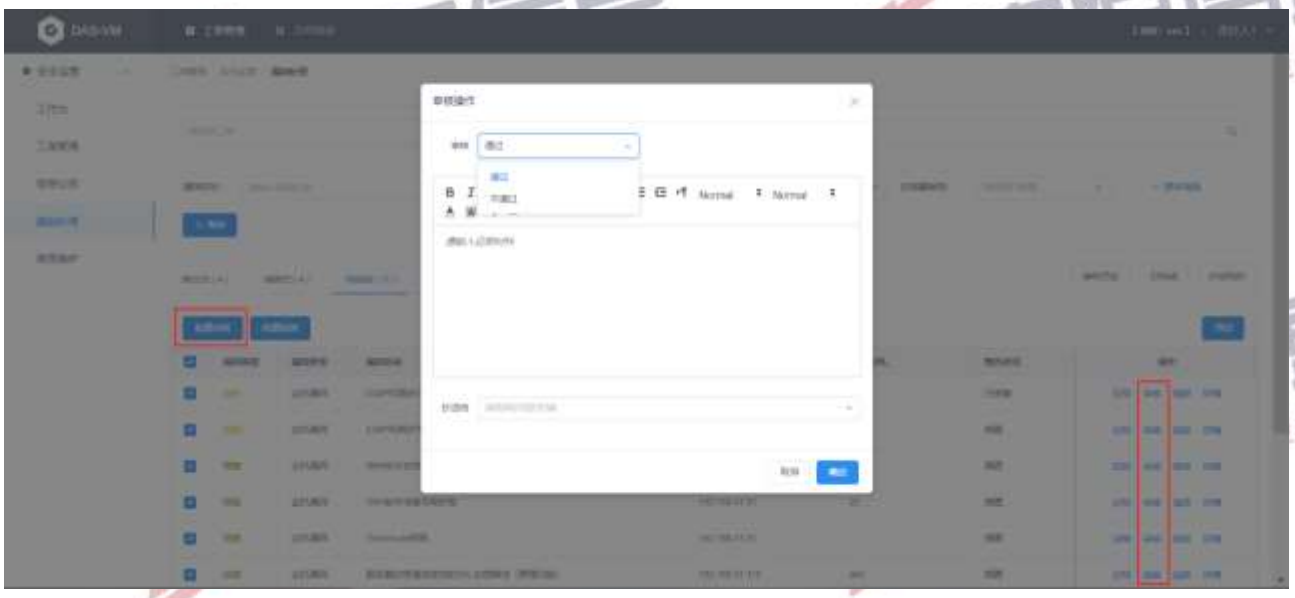


12.2.3.8. 审核漏洞

（1）拥有审核漏洞权限的责任人用户 WEB 登录后，进入工单系统[工单管理/安全运营/漏洞处理]页面，漏洞状态栏点击<待审核>查看待审核漏洞列表。

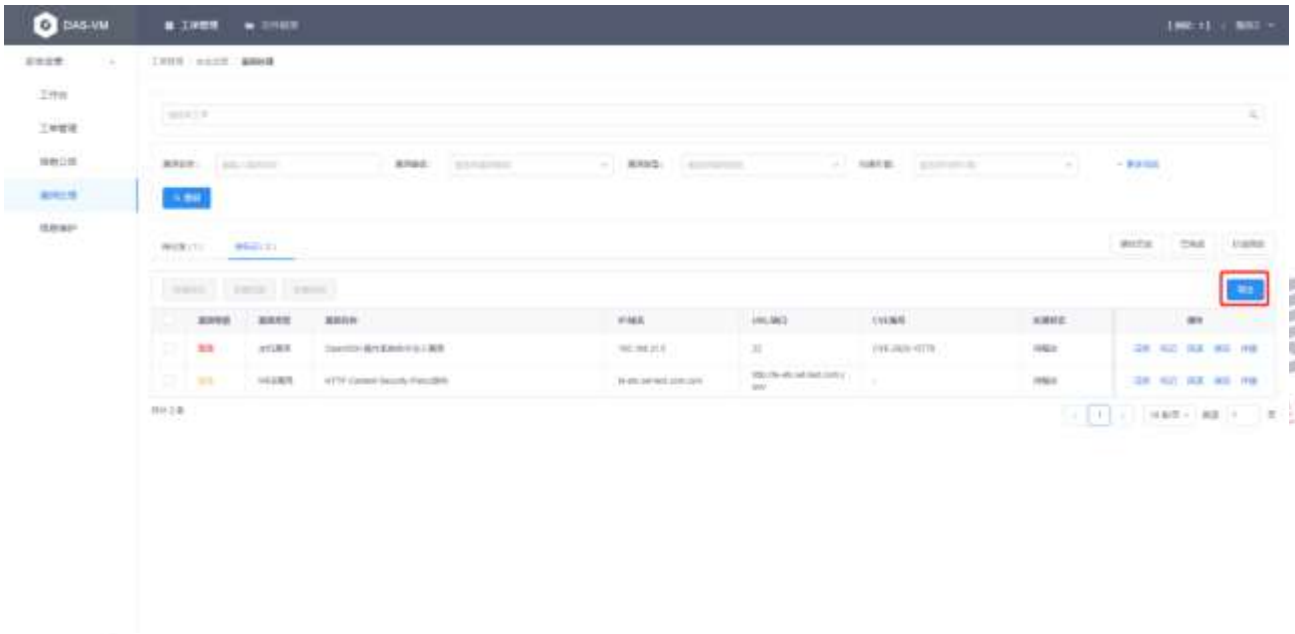


（2）待审核漏洞列表点击<审核>按钮或勾选多个漏洞点击<批量审核>按钮，选择审核通过或不通过，指定下一节点的人员，填写证明材料，点击<确定>按钮，若审核通过即可将漏洞提交给下一节点的人员，若审核不通过则将漏洞回退给上一节点提交漏洞的人员。若该节点下一节点为管理平台，则无需指定人员。若需要抄送其他人在抄送对象栏选择抄送对象。



12.2.3.9. 导出漏洞

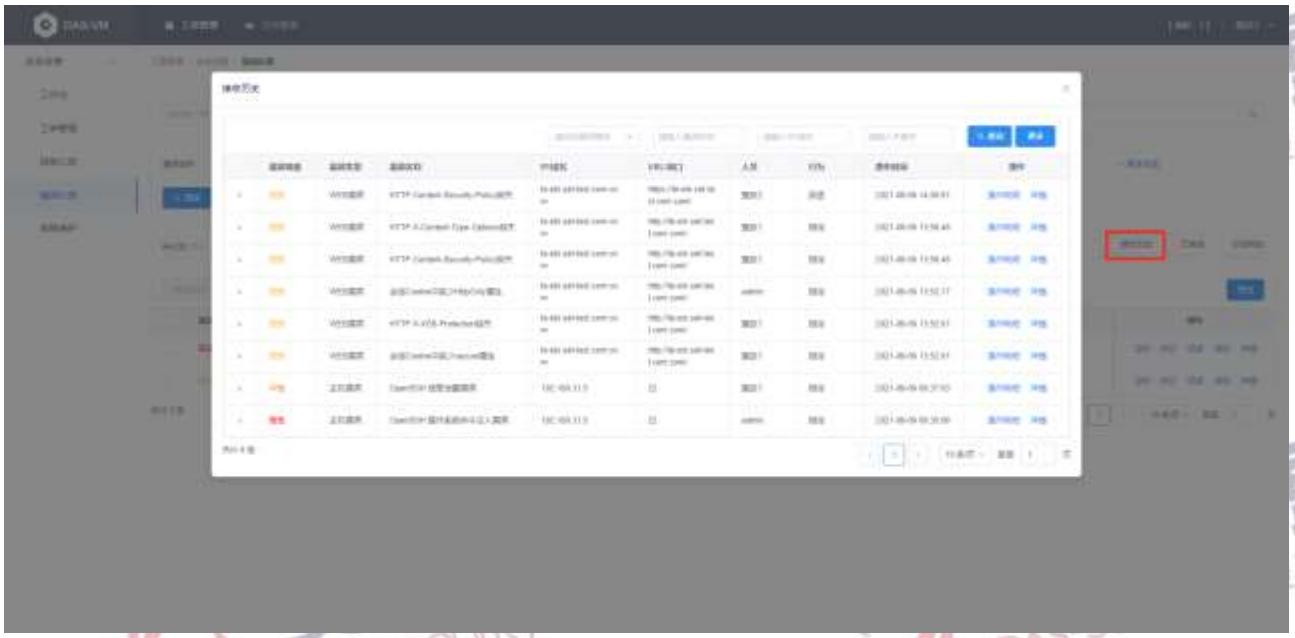
（1）点击<导出>按钮，可导出当前筛选条件（包括所选工单、漏洞查询条件、漏洞状态）下的漏洞列表。新增网页并自动跳转至工单系统的[文件报表/报表管理/下载管理]页面。



（2） 文件报表/报表管理/下载管理]页面点击下载列表中的<下载>按钮，可以下载列表中的相应报表。

12. 2. 3. 10. 接收历史

（1） 点击<接收历史>按钮展开当前登录用户的漏洞历史接收信息列表。



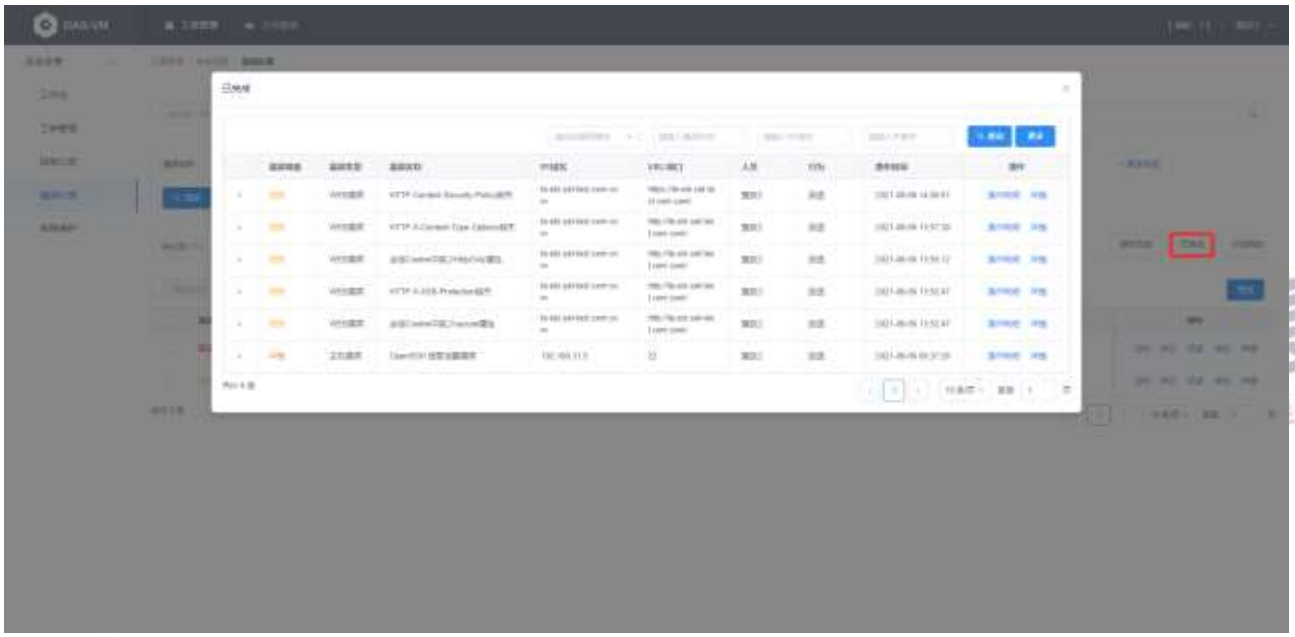
（2） 点击<操作明细>按钮展开对应操作时的证明材料。

（3） 点击<详情>按钮可查看漏洞的漏洞详情。

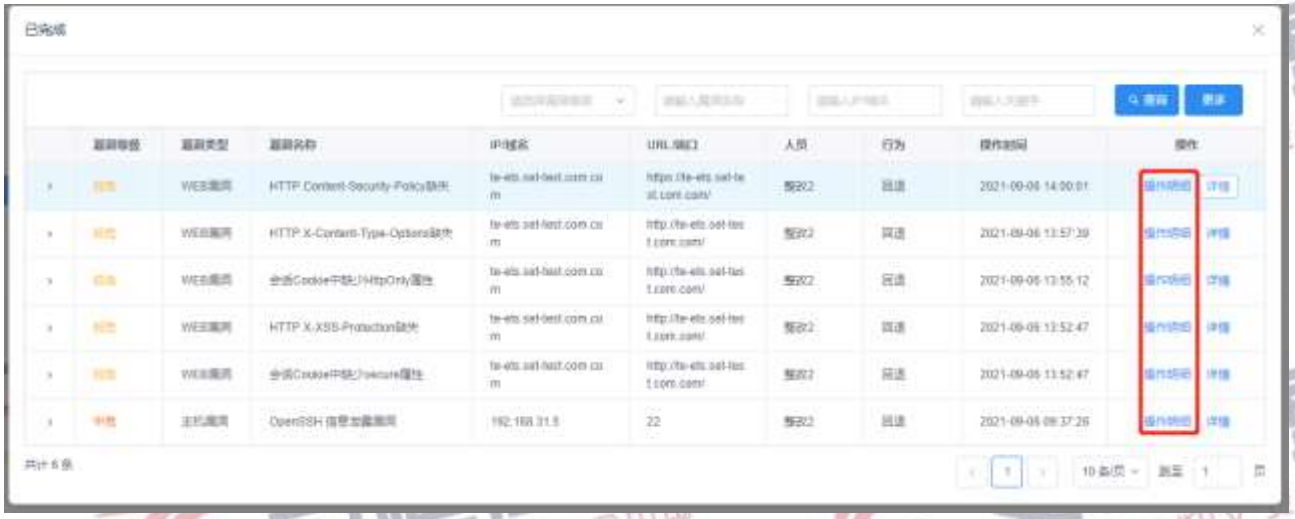
（4） 通过查询项可以查看相关接收漏洞。

12. 2. 3. 11. 已完成列表

（1） 点击<已完成>按钮展开当前登录用户的漏洞历史处理信息列表。



（2） 点击<操作明细>按钮展开对应操作时的证明材料。

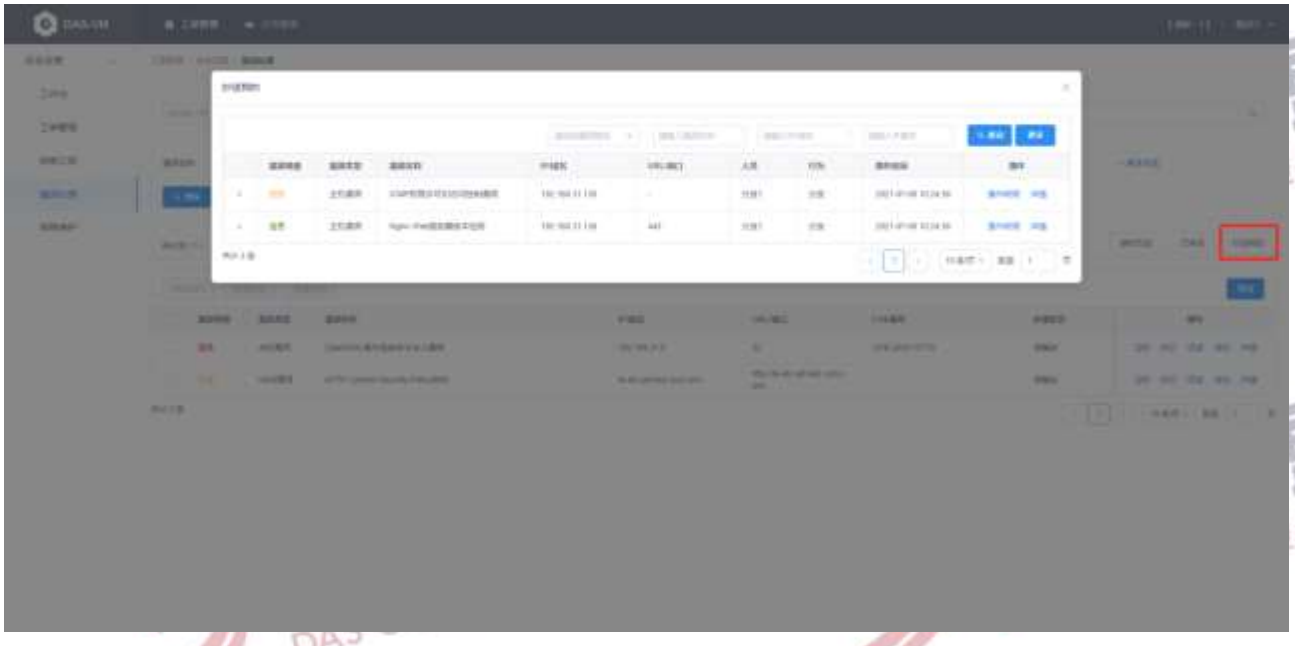


（3） 点击<详情>按钮可查看漏洞的漏洞详情。

（4） 通过查询项可以查看相关已完成漏洞。

12.2.3.12. 抄送列表

（1） 点击<抄送我的>按钮展开抄送当前登录用户的信息列表。



（2） 点击<操作明细>按钮展开对应操作时的证明材料。

（3） 点击<详情>按钮可查看漏洞的漏洞详情。

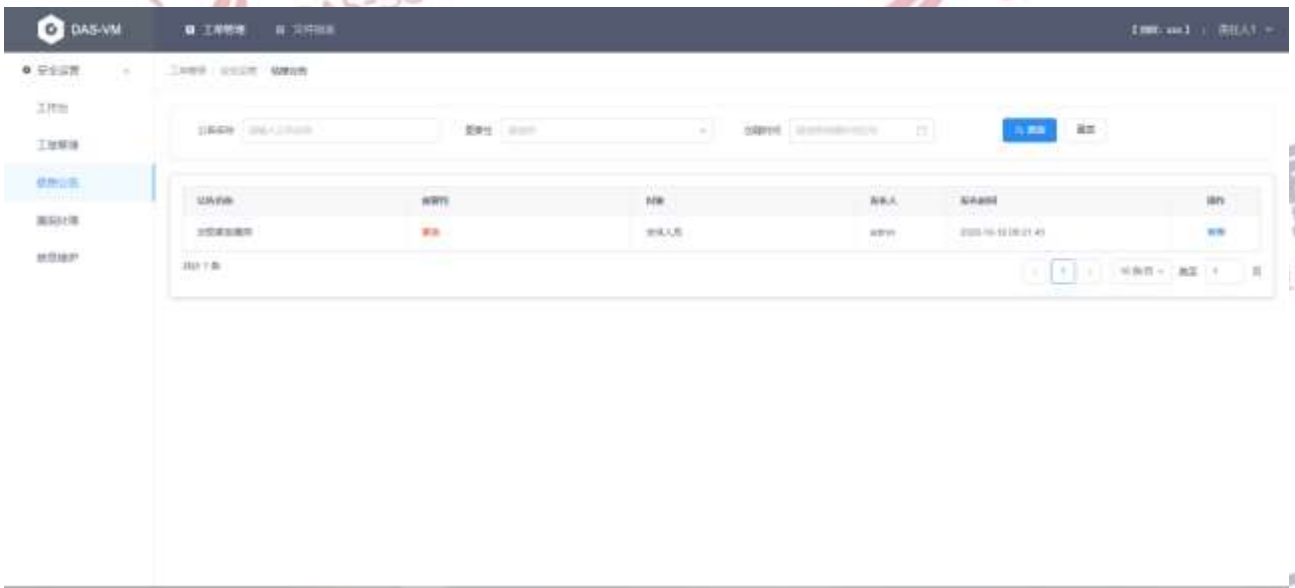
（4） 通过查询项可以查看相关抄送漏洞。

12. 2. 4. 信息公告

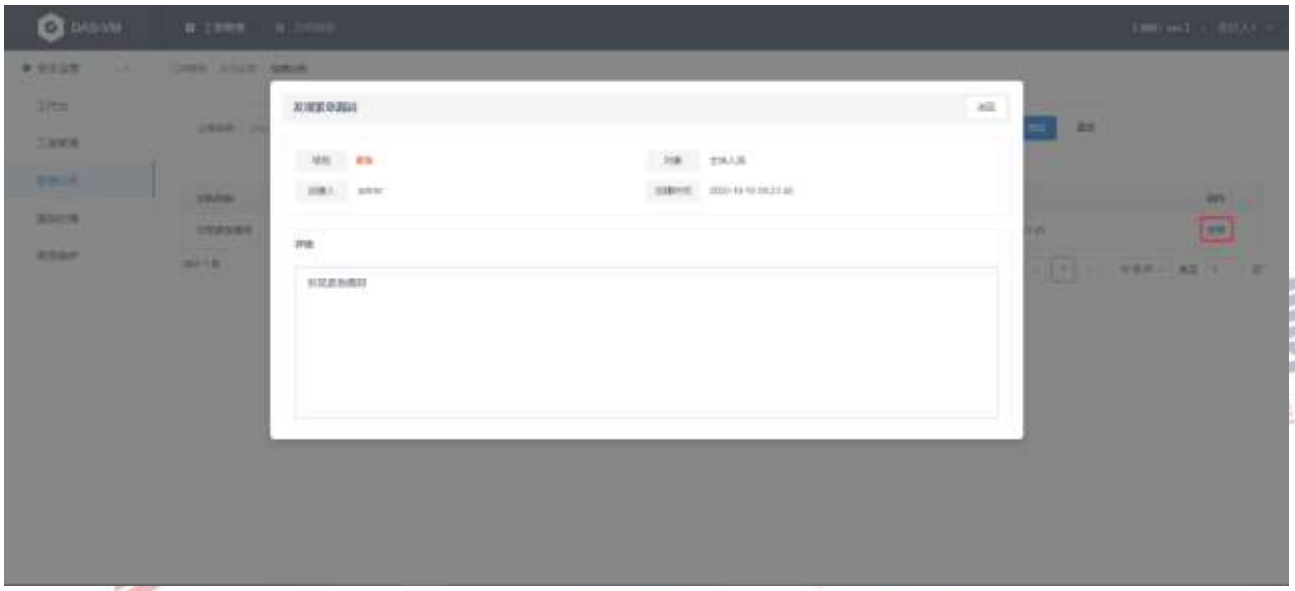
信息公告主要用于漏洞信息公告的查询和查看。

12. 2. 4. 1. 公告查看

（1） 责任人用户 WEB 登录后，进入工单系统[工单管理/安全运营/信息公告]页面。



（2） 点击信息公告列表中的<查看>按钮，弹出相应的信息公告详情框，可查看公告具体信息。



12.2.4.2. 公告查询

（1）设置查询条件，可在公告列表中进行指定公告查询，条件设置后，点击<查询>按钮，进行查询。点击<重置>按钮，可清空查询条件。

12.2.5. 信息维护

信息维护主要是用于工单系统用户的邮箱和登录密码修改。

12.2.5.1. 信息修改

（1）责任人用户 WEB 登录后，进入工系统[工单管理/安全运营/信息维护]页面，可查看当前登录用户信息。

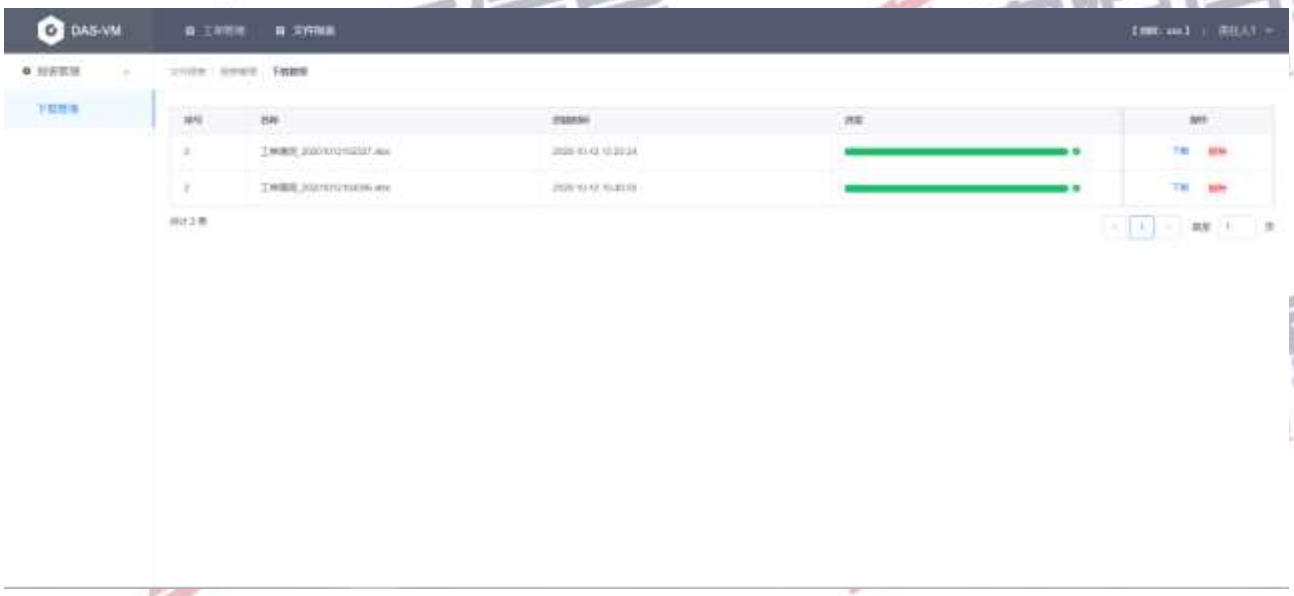
（2）输入要修改的邮箱地址，点击<修改密码>按钮，输入新密码，点击<提交>按钮，即可完成登录用户的邮箱和密码的修改。

12.3. 文件报表

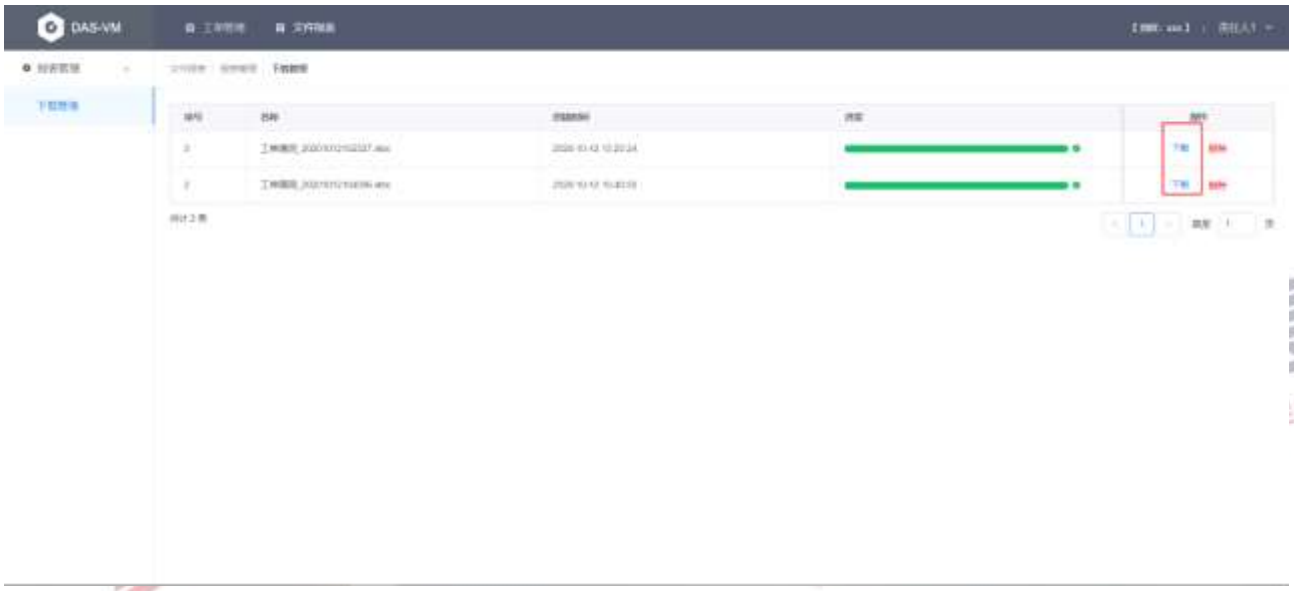
12.3.1. 下载管理

12.3.1.1. 下载报表

（1）责任人用户 WEB 登录后，进入工单系统[工单管理/报表管理/下载管理]页面。



（2）点击下载列表中的<下载>按钮，可以下载列表中的相应报表。



12.3.1.2. 删除报表

（1） 点击下载列表中的<删除>按钮并确定，可删除列表中的相应统计报表。