明鉴远程安全评估系统

用户使用手册

杭州安恒信息技术股份有限公司

V3.0.21

目录

1 声 明

1.1 版权声明

本文档包含了来自杭州安恒信息技术股份有限公司机密的技术和商业信息，提供给杭州安恒信息技术股份有限公司的客户或合作伙伴使用。接受本文档表示同意对其内容保密并且未经杭州安恒信息技术股份有限公司书面认可，不得复制、泄露或散布本文档的全部或部分内容。

本文档及其描述的产品受有关法律的版权保护，对本文档内容的任何形式的非法复制，泄露或散布，将导致相应的法律责任。

杭州安恒信息技术股份有限公司保留在不另行通知的情况下修改本文档的权利，并保留对本文档内容的解释权。

1.2 免责声明

本手册依据现有信息制作，其内容如有更改，恕不另行通知。杭州安恒信息技术股份有限公司在编写该手册的时候已尽最大努力保证其内容准确可靠，但杭州安恒信息技术股份有限公司不对本手册中的遗 漏、不准确或错误导致的损失和损害承担责任。

2 前言

2.1 文档范围

本文档覆盖明鉴远程安全评估系统（DAS-RAS）的功能点，并详细介绍 DAS-RAS 的主要功能模块的使用方法。

2.2 期望读者

期望了解本产品主要功能特性和使用方法的用户、系统管理员和网络管理员等。

2.3 内容简介

参考文档参见表 2-1。

表 2-1 内容简介

序号	标题	概述
1	版权声明	该文档的版权声明
2	前言	文档范围和格式约定等
3	产品简介	产品概述和功能简介
4	登录系统	登录方式和页面布局
5	系统管理	用户管理、告警配置、字典管理、引擎管理、许可管理、系统配置、系统服务、常用工具
6	资产管理	资产列表、授权管理
7	策略管理	网站策略、数据库策略、主机策略、基线策略
8	扫描任务	网站扫描、数据库扫描、基线配置核查、主机扫描
10	报表中心	综合报表、报告模板

2.4 获得帮助

如需获得网络安全以及产品相关资料，可以访问安恒信息技术网站：

http://www.dbappsecurity.com.cn/

由于产品版本升级或者其他原因，本文档内容会不定期进行更新。因此，如无特殊说明，本手册仅作为使用指导。

3 产品简介

3.1 产品概述

网络环境、信息系统架构越来越复杂，原本单一的检查工具已经渐渐不能满足弱点多样化的今天，用户越来越多的需要全方位的弱点发现能力。明鉴远程安全评估系统是一款融合安恒信息多年在信息安全漏洞挖掘、渗透测试技术研究和漏洞检查方法的最佳实践的基础上，集网络端口与服务扫描、

主机安全扫描、应用安全扫描于一身的功能，结合信息安全风险评估理论分析的综合安全技术扫描和管理系统。

该系统帮助用户有效的实现了漏洞扫描、配置核查的全生命周期管理，将技术和管理以及等级保护合规有效地融合在了一起，以管理系统的方式支撑用户单位信息安全整体工作，为用户单位信息系统整体风险评估提供有力的支撑。该产品 3.0 版本在 2010 年为上海世博会、广州亚运会 2011 年深圳大运会提供安全评估及服务，更是在 G20、世界互联网大会等国际性重要会议安保中发挥了重要作用。

3.2 综合扫描功能介绍

明鉴远程安全评估系统（DAS-RAS）功能主要包含了 Web、数据库、基线、主机扫描 4 大扫描功能，以及分布式集群扫描模块、统计报告控制体系、用户权限管理体系等辅助功能。

4 登录系统

4.1 登录方式

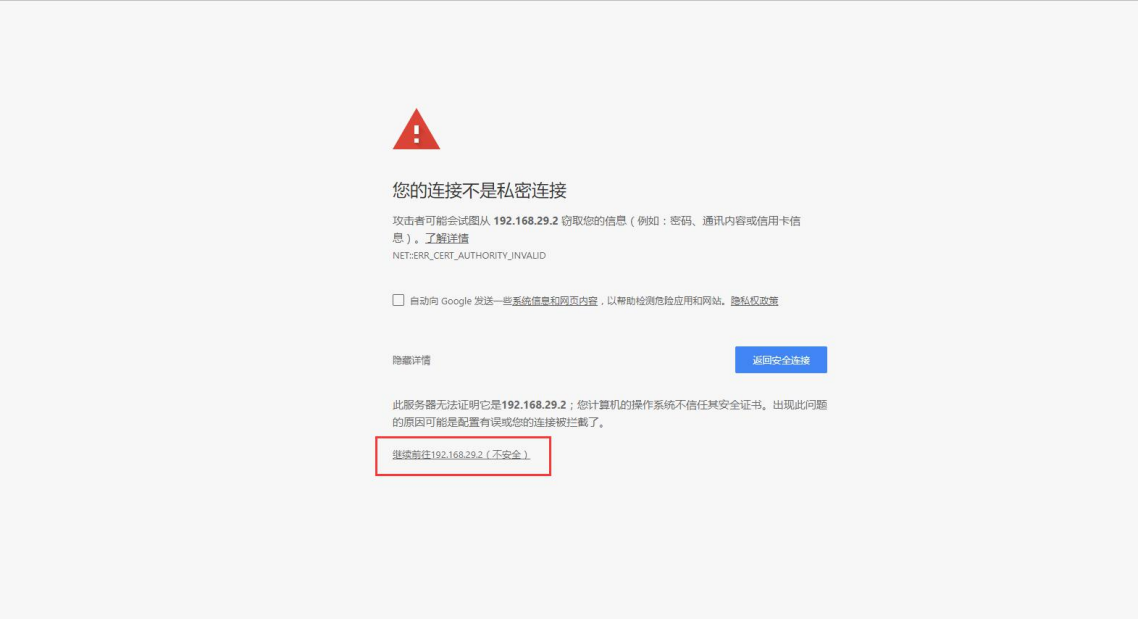
在浏览器中输入 *https://ip* 地址*:8891* ，在登录窗口中输入用户名、密码和验证码，进入登录窗口。如图 4-1 所示。（推荐使用chrome浏览器）

图 4-1 登录

点击{登录}后即可登录到整体概况页面。

首次使用　浏览器访问，提示此网站的安全证书存在问题，请选择“继续前往（不安全）”， 如图 4-2 所示。

图 4-2 首次 chrome登录提示



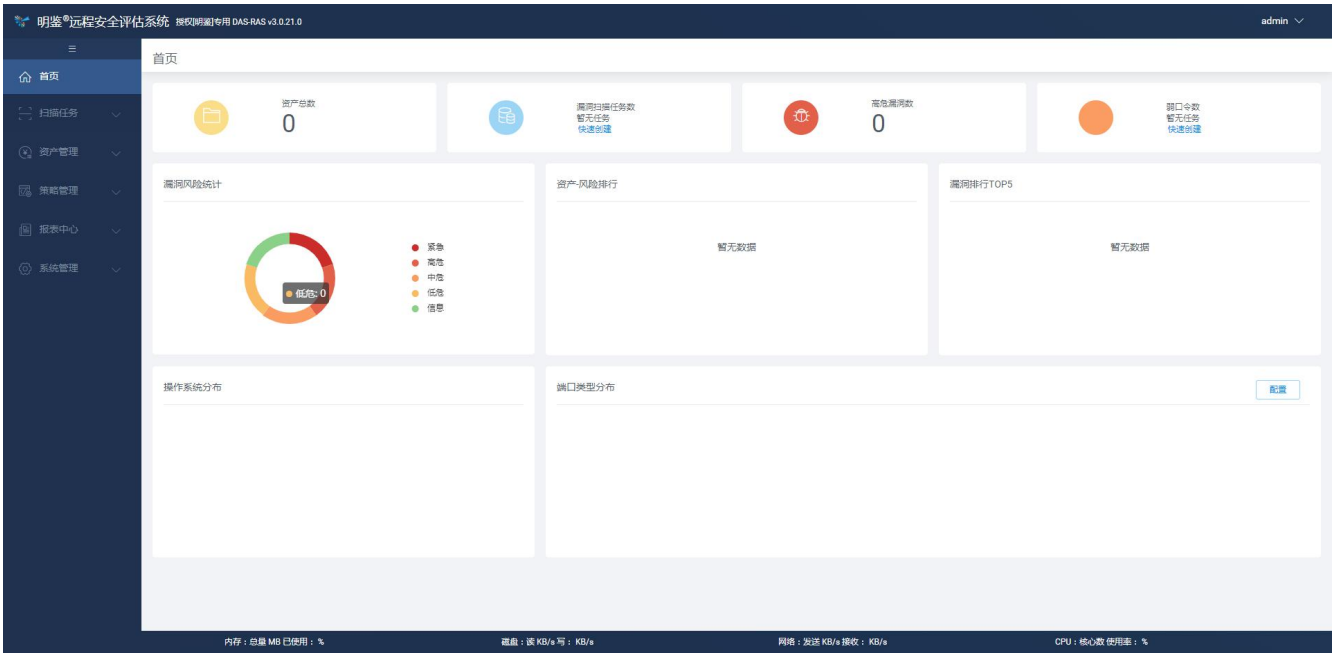
出厂默认访问 IP 为：*192.168.1.100*
出厂默认用户名/密码为：

admin/yc49pG.No1　　（用户管理员）
auditor/yc49pGa.No1　（系统审计员）
operator/yc49po.No1　（系统操作员）

4.2 页面布局

登录后的整体页面如图 4-3 所示。

图 4-3 整体页面



4.2.1 菜单栏

以树形结构方式，显示各种功能的菜单，如图 4-4 所示。

图 4-4 菜单栏

由于新版的远程评估系统三权分立，原先的系统管理功能模块被移到了 admin（用户管理员）下面。

4.2.2 状态栏

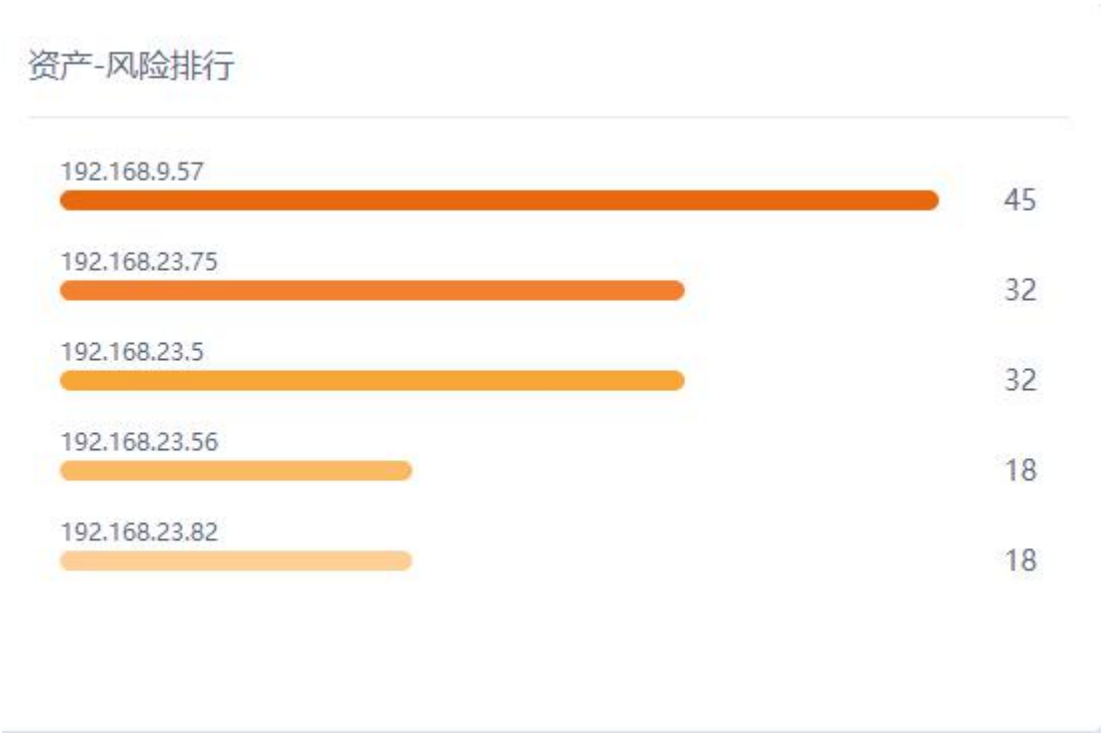
以图形的形式，显示资产总数和快速创建任务，如图 4-5 所示。

图 4-5 状态栏

4.2.3 风险消息

根据左上角的按键可切换显示网站扫描、数据库扫描、基线扫描的风险消息，如图 4-6 所示。

图 4-6 资产风险信息



4.2.4 漏洞风险完全统计、漏洞排行、操作系统及端口类型分布

在首页中可以显示漏洞风险完全统计，如图 4-7 所示

在首页中可以显示漏洞排行TOP5的信息，如图 4-8 所示

在首页中可以显示操作系统分布及端口类型分布信息，如图 4-9 所示


漏洞风险完全统计
中危: 109
紧急
高危
中危
低危
信息

图 4-7


漏洞排行TOP5
检测目标主机WEB服务器信息
25
OpenSSH sshd monitor.c文件权限许可和访问控制漏洞
12
OpenSSH 'x11_open_helper()' 函数权限许可和访问控制漏洞
12
OpenSSH sshd monitor组件输入验证漏洞
12
OpenSSH sshd 权限许可和访问控制漏洞
12

图4-8

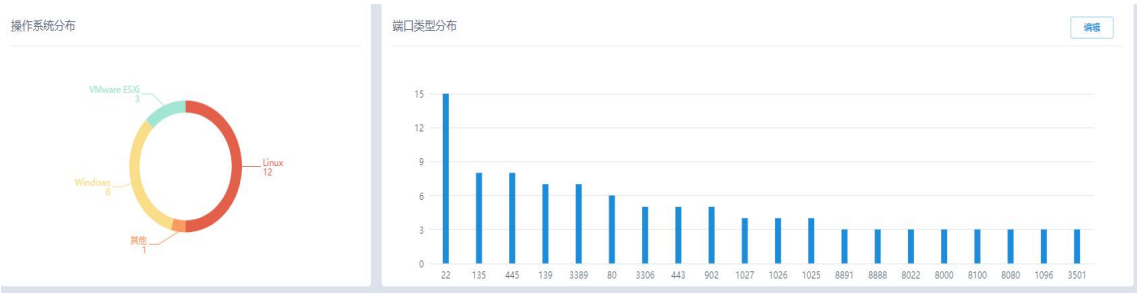

操作系统分布
端口类型分布
编辑
VMware ESXi
3
Linux
12
Windows
8
其他
1
15
12
9
6
3
0
22
135
445
139
3389
80
3306
443
902
1027
1026
1025
8891
8888
8022
8000
8100
8080
1096
3501

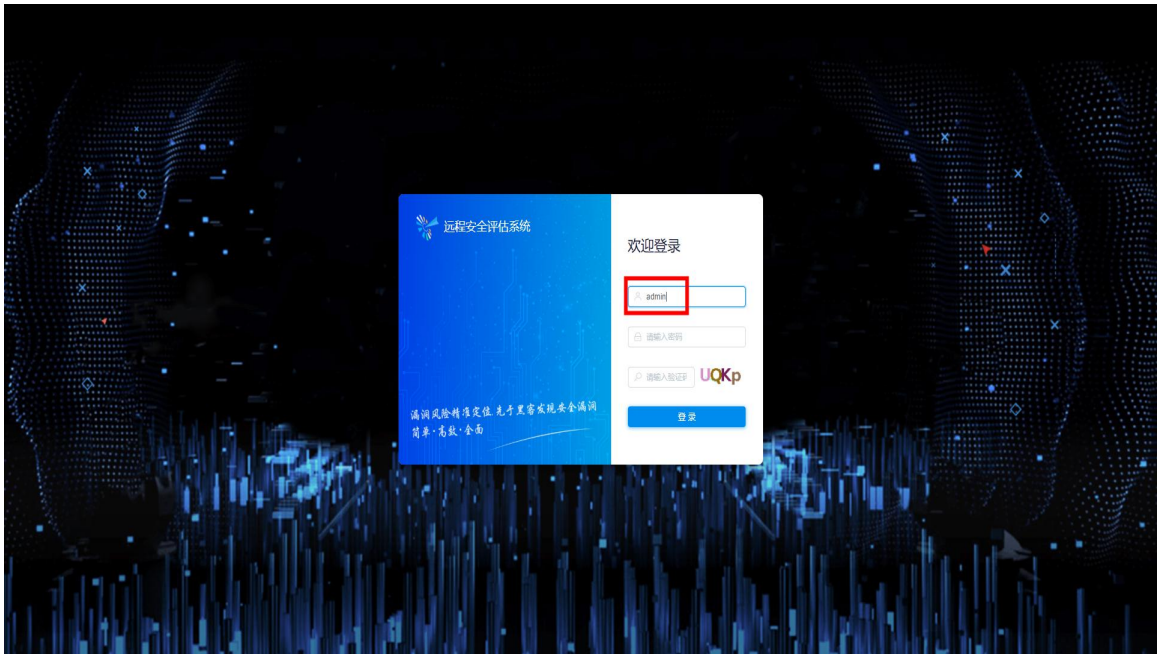
图4-9

4.3 用户管理

用户管理功能可以建立不同角色和部门的用户，并对用户进行编辑、禁用和删除等操作。管理员需通过切换账户的形式实现，管理员登录通过 admin，打开用户管理界面。

登录界面如图 4-10

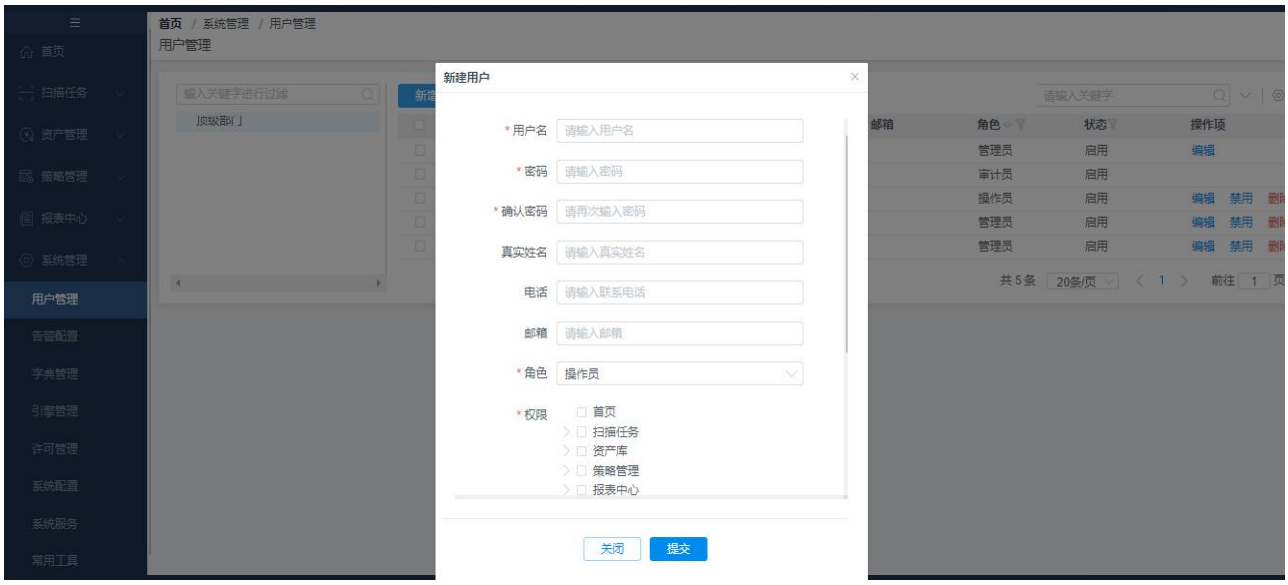
图 4-10 登陆



4.3.1 新建用户

新建用户界面如图 4-11 所示。

图 4-11 新建用户



新建用户输入项说明见下表 4-1。

表 4-1 新建用户输入项

序号	输入项	说明	是否必填
1	用户名	用户名只能是3-14位字符，支持数字、字母和下划线,'.'任意组合。	是
2	密码	支持8-20位数字、字母和特殊字符(空格)的任意组合。	是
3	确认密码	同密码一致。	是
4	角色	管理员在增加用户时，需要给用户指定一个角色，系统只内置三种默认角色，分别为：管理员、审计员和操作员。	是
5	部门	默认显示顶级部门，可选择用户自定义部门。	是
6	真实姓名	显示该用户的真实姓名	否
7	电话	注册用户的联系方式	否
8	邮箱	注册用户的联系邮箱	否
9	有效期	该账户可用时间节点	是
10	权限	设置该用户的使用权限	是
11	允许扫描范围	设置该账户的允许扫描范围	否

默认三种角色：管理员、审计员和操作员。

输入所有必填选项后，点击【提交】，用户成功添加后显示在用户列表中。

4.3.2 修改用户

管理员用户点击 

按钮，可编辑用户的角色、部门，
可修改密码等，如图 4-12所示。

图4-12

4.3.3 删除用户

点击 

，可删除对应用户，如图 4-13 所示。

图 4-13 删除用户

删除后的用户不可再登录。

删除后可新建与删除用户名一致的用户。

4.3.4 禁用和启用用户

点击 禁用 ，可禁用对应用户，如图4-14所示。

图4-14

禁用后的用户不可登录。

重新启用后可以登录。

禁用的用户，点击 启用 ，可恢复正常状态。

4.4 新建部门

部门可以添加、修改和删除部门。

管理员点击 可以直接进行添加。如图 4-15、4-16

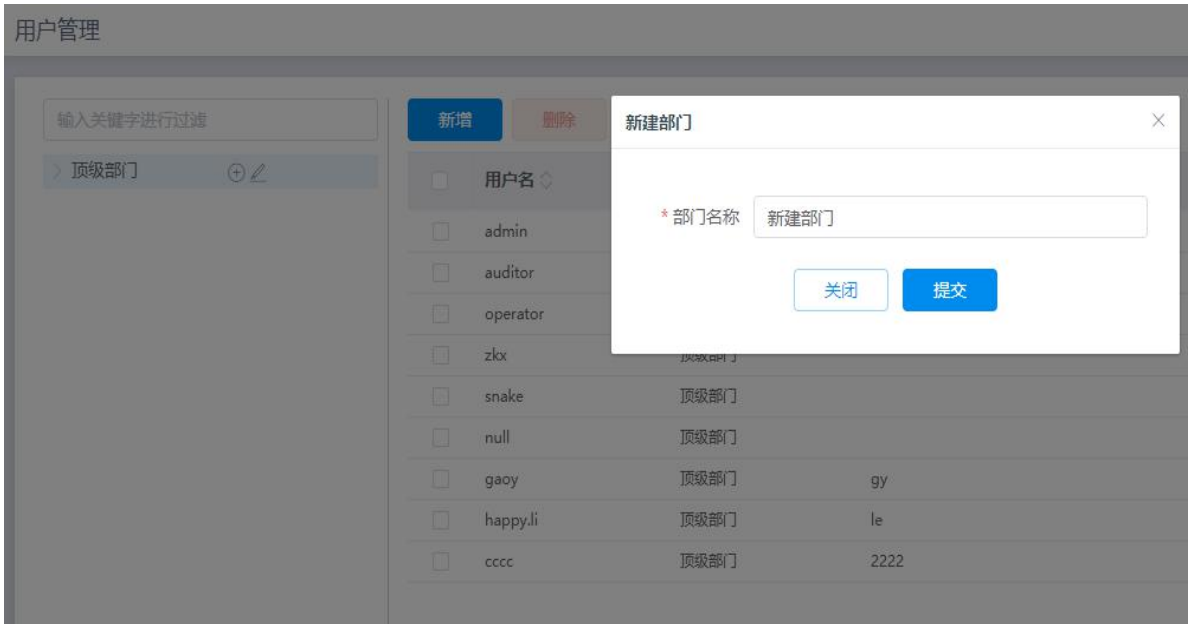


图4-15

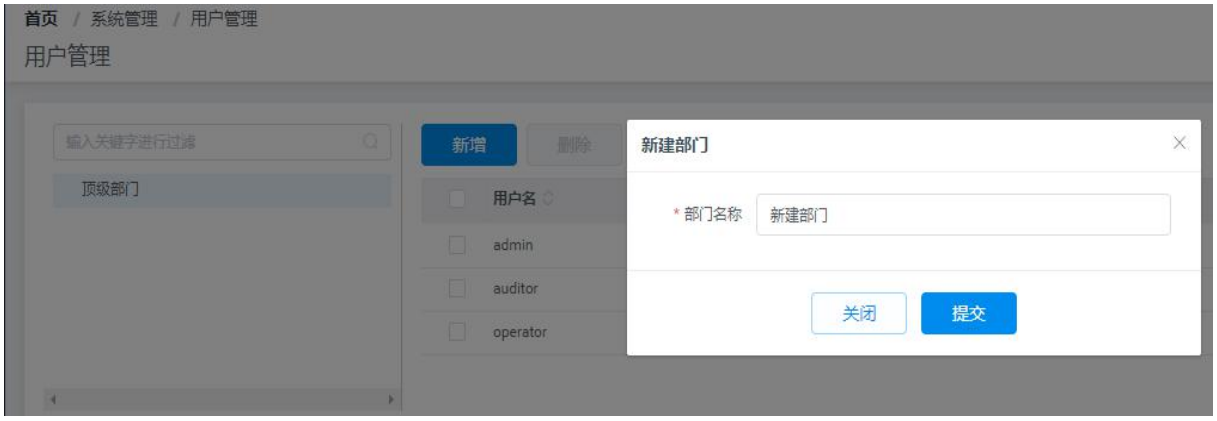


图4-16

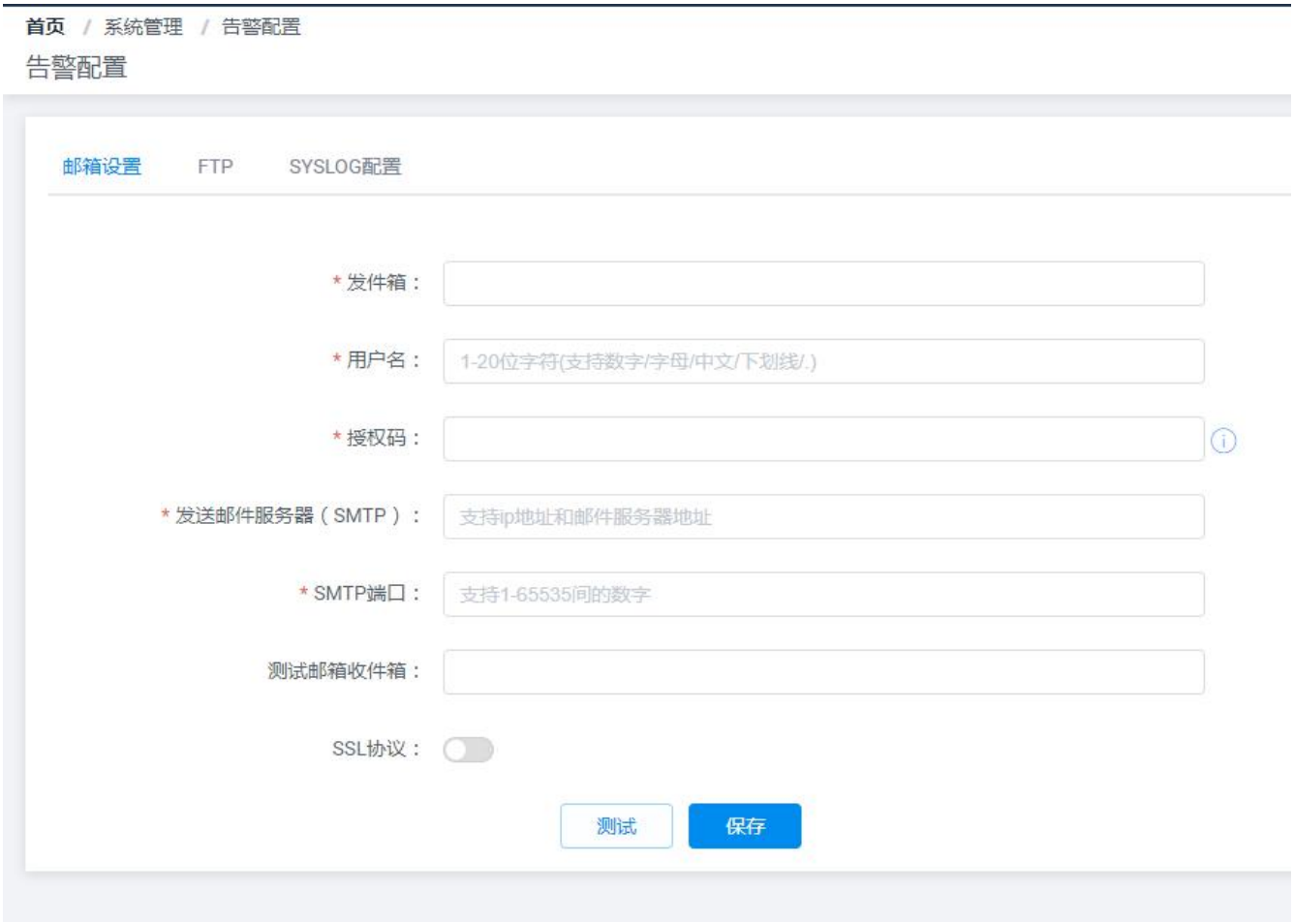
一个部门可以查看自己与下级部门资源，不可以查看其他部门资源。

默认顶级部门，顶级部门不可修改和删除。

4.5 告警设置

点击【系统管理】---【告警配置】---【邮箱设置】，打开邮箱配置界面，如图 4-17 所示。

图 4-17 邮箱配置



邮箱配置输入项说明见下表 4-5。

表 4-5 邮箱配置输入项

序号	输入项	说明	是否必填
1	发件箱	即发件箱的地址。	是
2	用户名	发件箱的用户名，支持1-20位字符。	是
3	授权码	用于登录第三方客户端的专用密码。	是
4	发送邮件服务器(SMTP)	发送邮件服务器的IP地址。	是
5	SMTP端口	该服务器的端口号，支持1-65535间数字。	是
6	测试邮箱收件箱	用于进行测试设置是否成功的收件箱。	否
7	Ssl协议开关	可以选择是否开启ssl协议	否

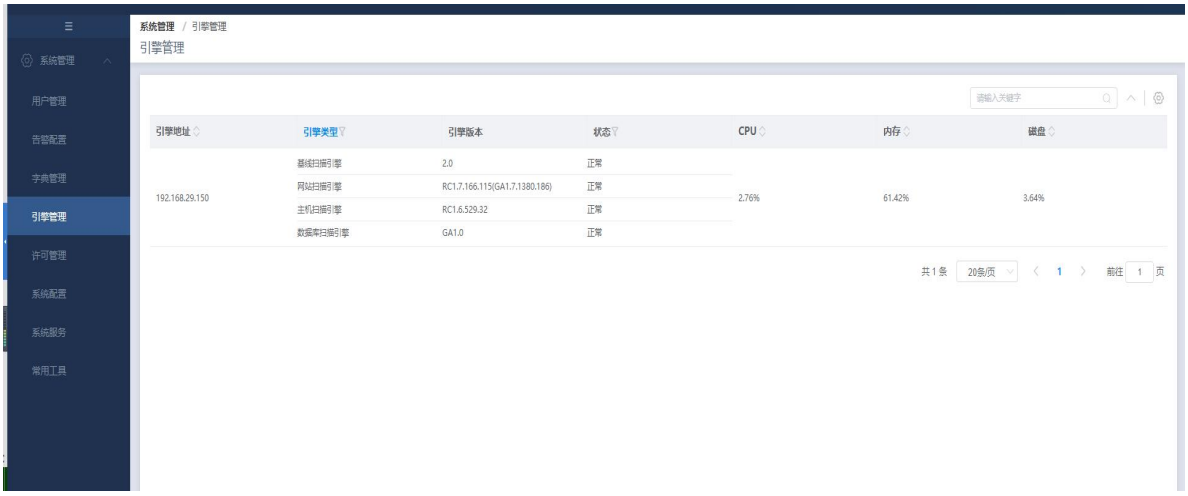
输入邮箱配置信息后，点击【测试】，可以测试所填邮箱是否可正常连接，点击保存，可保存邮箱配置信息。

4.6 引擎管理

引擎管理功能可以查看引擎名称、引擎地址、引擎版本、引擎类型、状态，并根据需要进行筛选查看。

管理员通过 admin 账户登陆，点击【引擎管理】，打开引擎管理界面。如图 4-18 所示

图 4-18 引擎管理



4.6.1 查看和查询引擎

在引擎列表中可以查看引擎基本信息，如图 4-19 所示，显示引擎地址、引擎类型、状态、使用率。可以输入引擎类型、引擎地址、状态，查询符合条件的引擎信息。

图 4-19 查看及查询引擎信息

4.7 字典管理

字典管理是用于上传用户名和密码的字典，用户可自定义设置弱口令的用户名和密码字典，创建弱口令扫描任务时，可以选择自定义的用户名和密码字典。如图所示 4-20 所示。

图 4-20字典列表

4.8 许可管理

许可管理能查看许可的各种信息，包括系统当前许可有效期、许可授权信息和许可使用限制信息。也能导入新许可。如图 4-21 及 4-22 所示许可授权信息。

4.8.1 查看许可信息

图 4-21 许可有效期

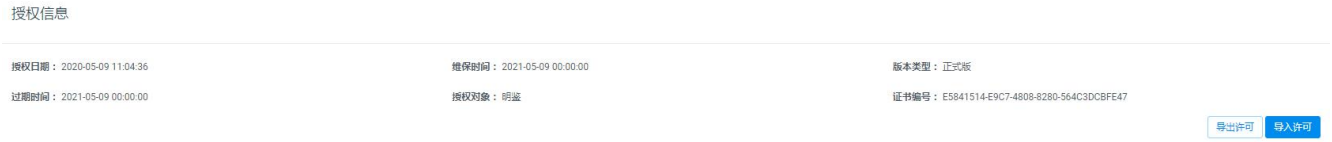


图 4-22 许可使用限制

4.9 系统设置

4.9.1 网络配置

系统网络配置如图 4-23 所示，显示状态描述，网卡名称，物理地址，IPV4 地址，IPV4子网掩码，,IPV4网关，IPV6地址，IPV6网关，开机启动和操作项。

图 4-23 网络配置

点击 编辑 可修改 IP 地址，子网掩码和开机启动项，如图 4-24 所示。

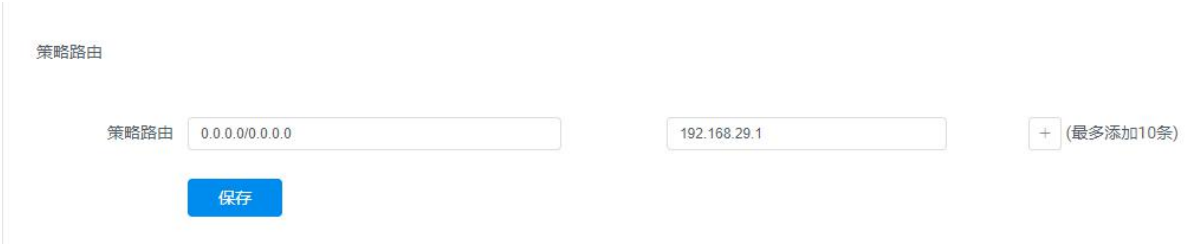
图 4-23 编辑网络配置

修改完网络配置后，会造成该条网络（约一分钟）不能访问。

4.9.2 策略路由配置

配置界面如图 4-25 所示。

图 4-25 默认网关及策略路由配置



策略路由输入项说明见下表 4-6。

表 4-6 策略路由输入项说明

序号	输入项	说明	是否必填
1	策略路由	从目的网络到下一跳网络，最多可添加4条。目的网络格式为x.x.x.x/xx或x.x.x.x/x.x.x.x。	否
2	下一跳	下一跳网络格式为x.x.x.x。	否

输入策略路由，点击【保存】，策略路由成功保存在列表信息中。

4.9.3 DNS 配置

配置界面如图 4-26 所示。

图 4-26 DNS 配置

DNS 配置输入项说明见下表 4-7。

表 4-7 DNS 配置输入项说明

序号	输入项	说明	是否必填
1	首选DNS服务器	DNS地址	是

2	备选DNS服务器	DNS地址	是

4.9.4 安全配置

配置界面如图 4-27 所示。
登陆失败处理方式有三种：1 不处理、2 锁定账户、3 锁定 IP；默认不处理

图 4-27 安全配置

表 4-8 安全配置说明

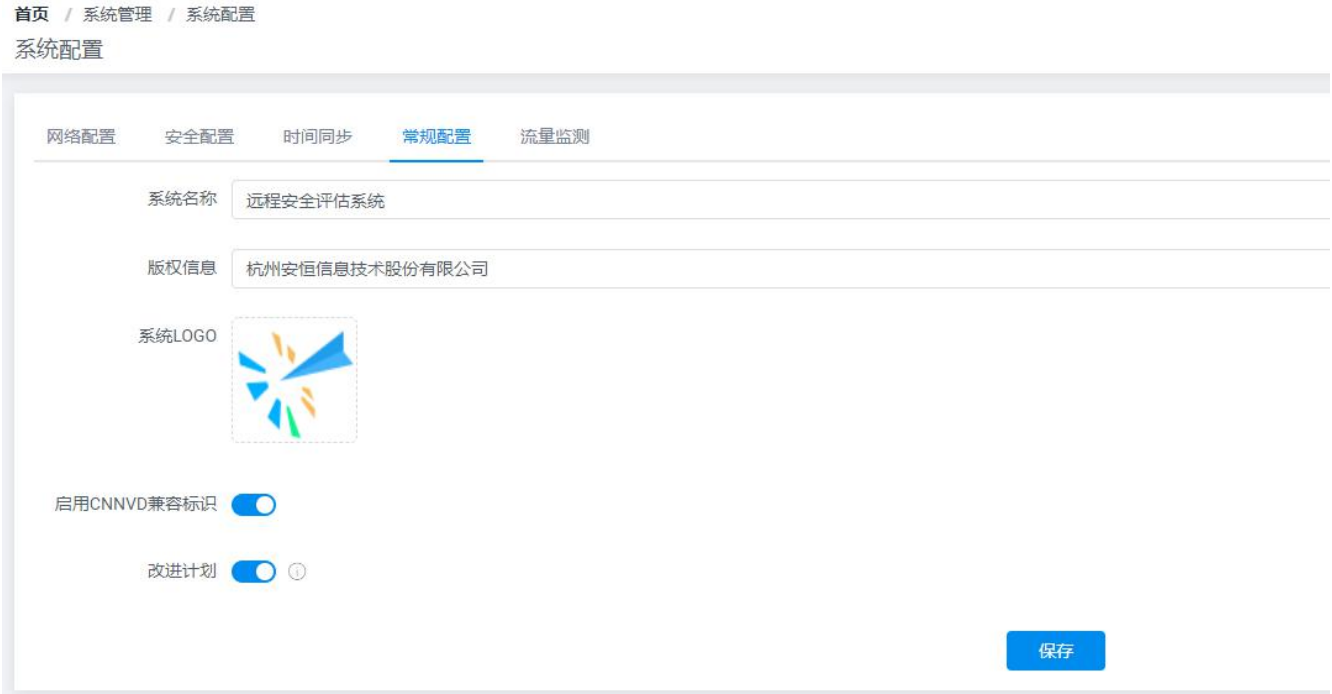
序号	输入项	说明	是否必填
1	最小密码长度设置	1-2位字符（支持大于7且小于等于20的数字，不得大于密码最大长度）。	是
2	最大密码长度设置	1-2位字符（支持大于7且小于等于20的数字，不得小于密码最小长度）。	是
3	密码强度设置	可以选择数字、字母（大小写）、特殊字符进行组合。	否
4	密码更换周期	1-2位字符（支持大于0且小于等于30的数字）	是
5	登录失败锁定方式	可按需要选择不处理、锁定账户、锁定ip方式	是
6	登录验证码	选择开关（默认开启，可选择关闭）	是
7	磁盘状态告警配置	可选择40%-95%等百分比	是
8	超时自动退出配置	1-2位字符（支持大于等于0，小于等于60以内的数字，且设置为0是为不超时登出）	是
9	是否启用访问控制	选项是否开启	否

4.9.5 时间同步

用于同步当前系统时间，可通过网络获取系统时间和手动设置系统时间，以确保当前系统不会存在较大的误差；具体配置如图所示：

4.9.6 常规配置

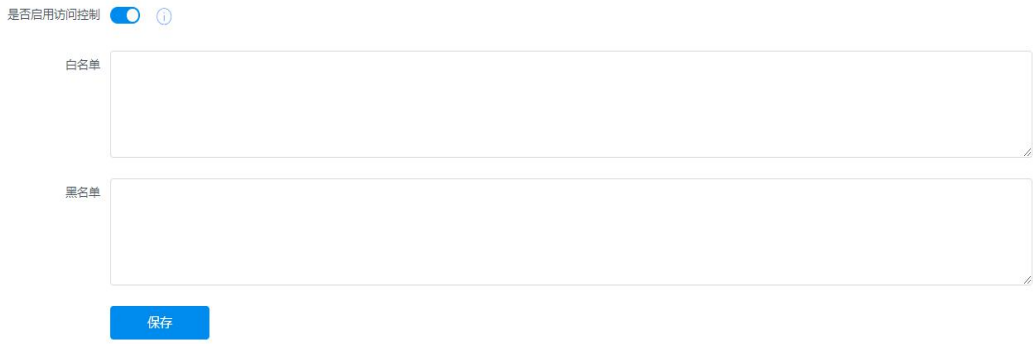
此配置用于针对需要自定义产品名称和公司名称等信息的设置选项，其中包含了：系统名称、版权信息、系统logo、是否启用CNNVD兼容性标识；



4.9.7 访问权限控制

访问权限控制界面如图 4-28 所示，显示有是否启用权限控制，黑/白名单，白名单 IP 和黑名单 IP。

图 4-28 访问权限控制



访问控制权限输入项说明见下表 4-9。

表 4-9 访问控制权限输入项说明

序号	输入项	说明	是否必填
1	是否启用访问控制	可选择启用或者不启用，不启用该功能时，默认所有的IP均可访问系统。当启用访问控制时，黑/白名单才可以选择和输入。默认不启用	否

2	黑/白名单	仅白名单启用时，只有白名单中IP可以访问系统；仅黑名单启用时，只有黑名单中的IP不可以访问系统；黑白名单同时启用时，除黑名单中的IP外的白名单IP可以访问系统（例如：白名单中192.168.1.*，黑名单中为192.168.1.222，则表达除192.168.1.222以外的192.168.1.*网段IP均可访问系统）	否
3	白名单	白名单IP，可以是IP地址或者是IP范围，例如192.168.1.*或者192.168.1.222	否
4	黑名单	黑名单IP，可以是IP地址或者是IP范围，例如192.168.1.*或者192.168.1.222	否

4.9.8 系统服务

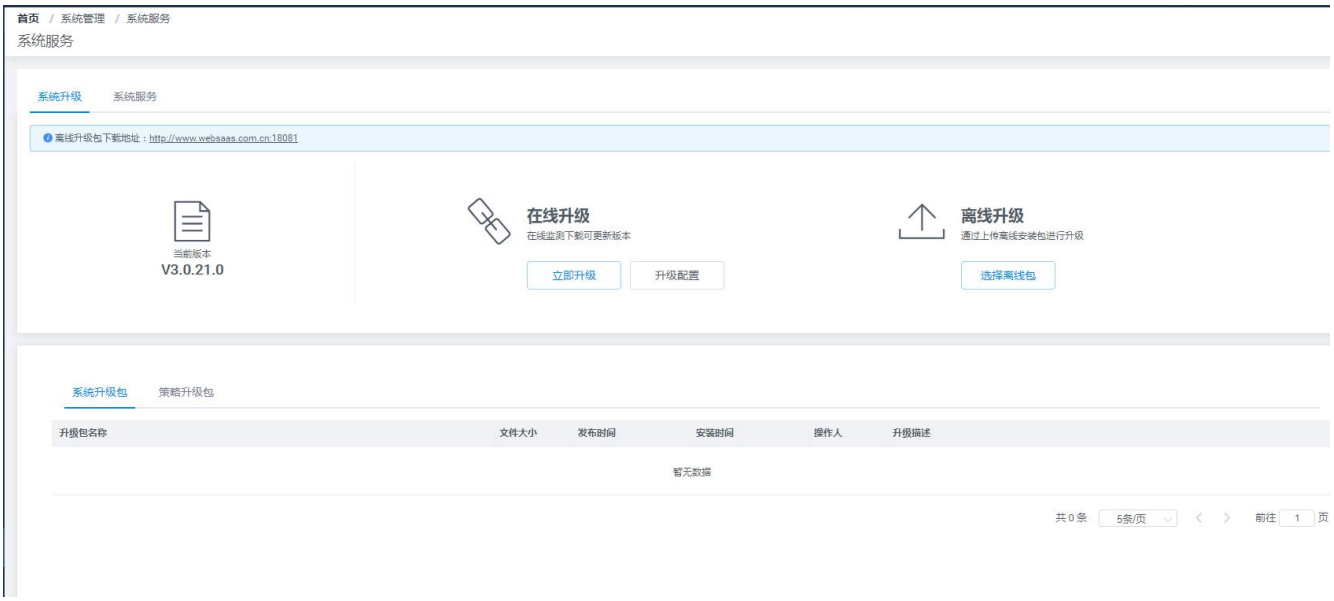
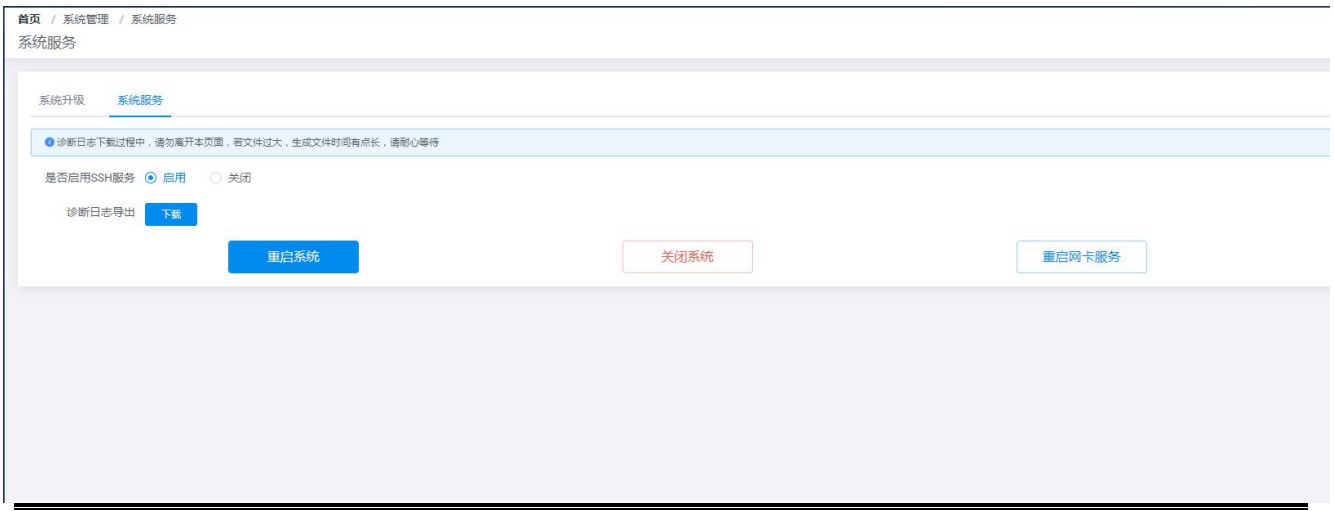


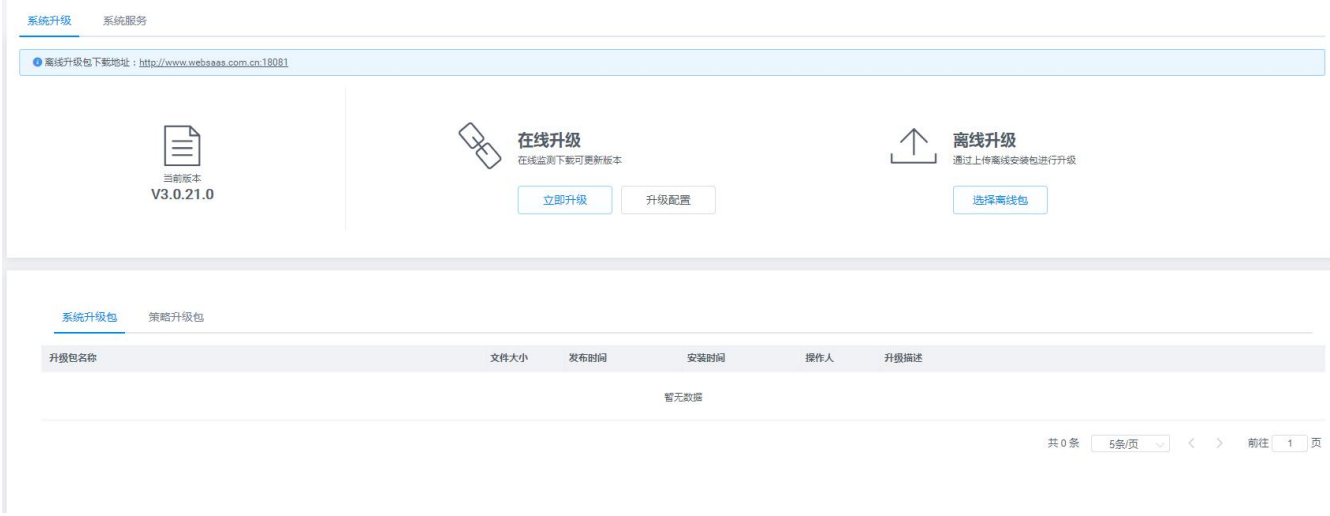
图 4-29 系统服务

系统服务可重启计算机，重启网卡服务，关闭系统。如图 4-30所示。

图 4-30 系统服务



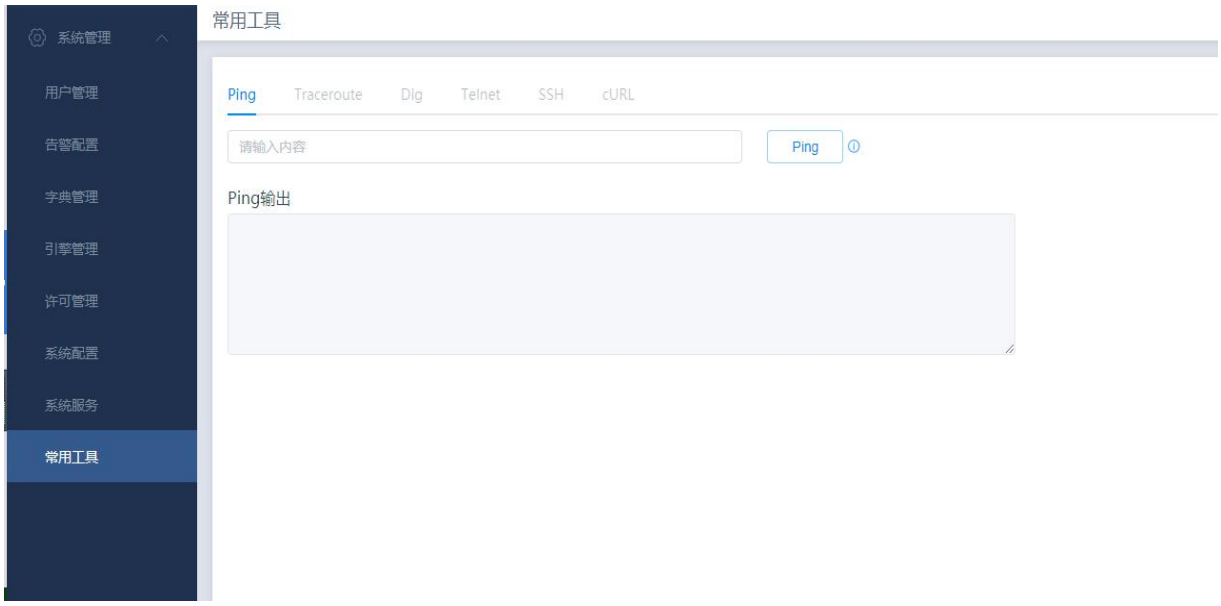
系统升级包含版本信息查看、在线升级、离线升级，如图 4-31 所示。



4.10 常用工具

常用工具中有Ping、Traceroute、Dig、Telnet、SSH、Curl 6 种日常经常会用到的工具供用户使用，如图 4-32 所示。

图 4-32 常用工具



5 资产管理

扫描的基本流程为：新建资产→选择策略→下发扫描任务→查看扫描结果→导出统计报告。

资产包括创建的网站资产和主机资产。

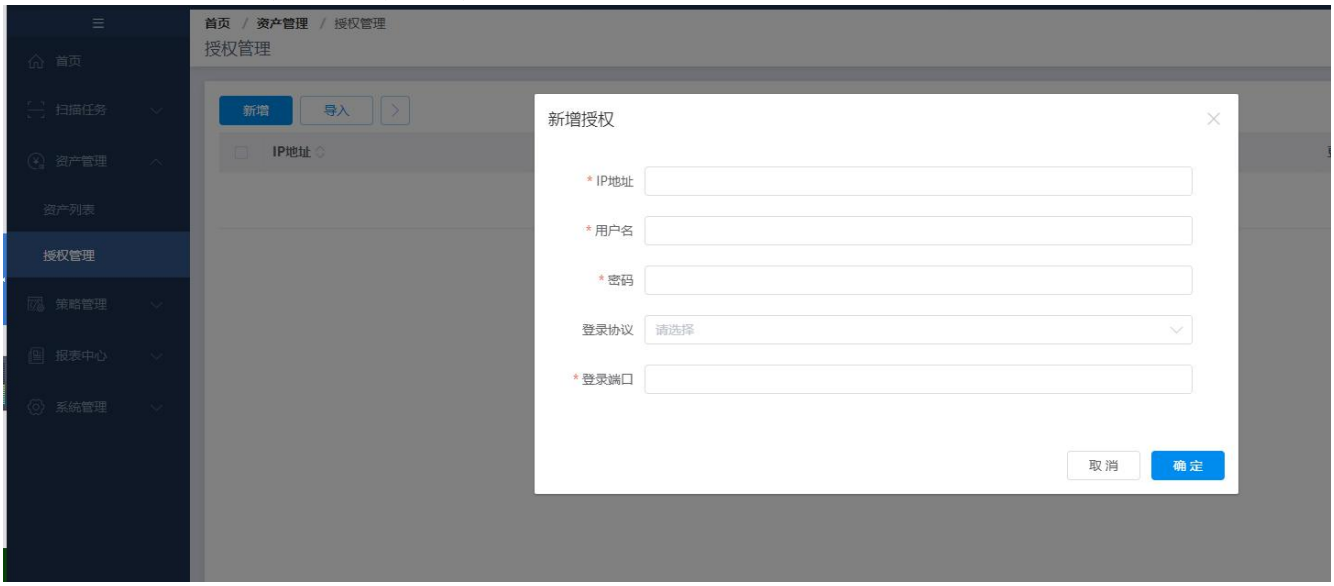
5.1 资产列表

新建主机资产 图5-1

新增网站资产 图5-2

5.2 授权管理

此项可添加授权登录资产IP 信息，图5-3



6 策略

6.1 网站策略

操作员用户根据已有的网站策略，创建策略分组，在新建网站扫描任务时，可以选择策略组进行漏洞扫描。

点击【策略管理】→【网站策略】，在左侧显示按照默认类别分组的策略，每个类别后的数字代表策略条数，如图 6-1 所示。点击不同的类型，在右侧列表中显示不同的策略。

图 6-1 网站策略分组类别显示

网站策略默认分组内容显示如图 6-2 所示。

6.2 数据库策略

操作员用户根据已有的数据库策略，创建策略分组，在新建数据库扫描任务时，可以选择策略组进行数据库扫描。

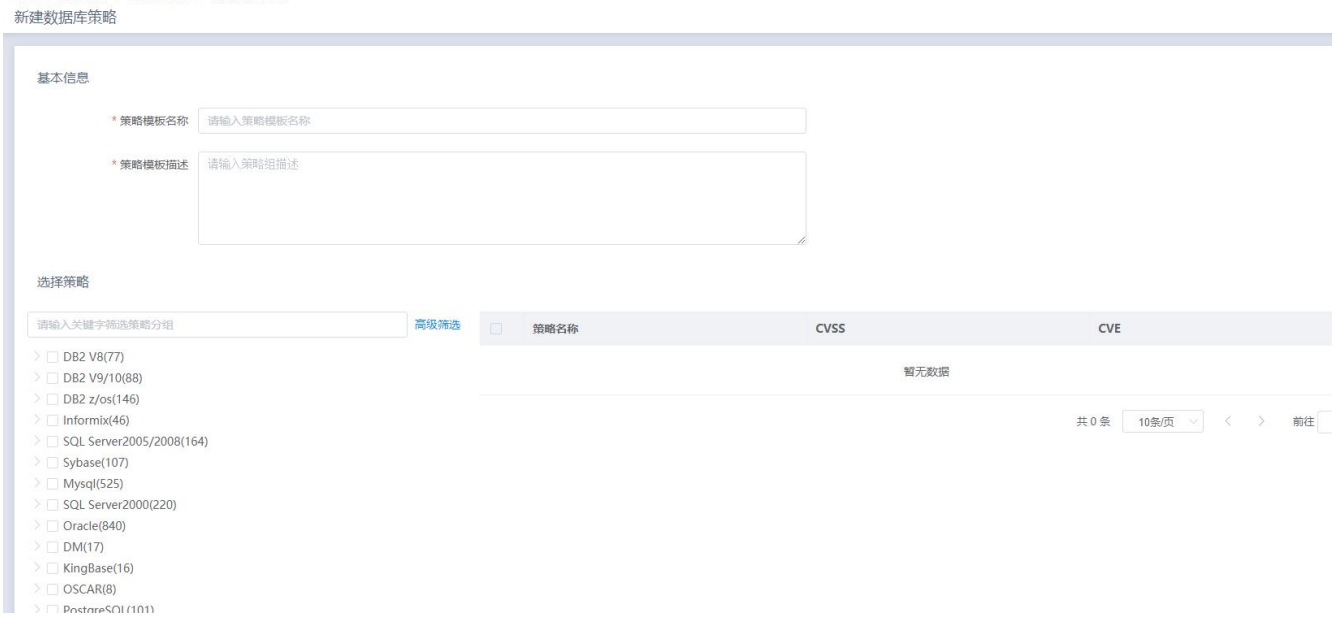
点击【策略管理】→【数据库策略】，如图 6-3 所示。点击不同的类型，在右侧列表中显示不同的策略分组。

图 6-3数据库策略分组显示

数据库策略默认分组显示如图 6-4 所示。

图 6-4数据库策略默认分组内容

图 6-5 自定义策略分组



6.3 基线策略

操作员用户根据已有的基线策略，创建策略分组，在新建基线扫描任务时，可以选择策略组进行基线扫描。

点击【策略管理】→【基线策略】，如图 6-6 所示。点击不同的类型，在右侧列表中显示不同的策略分组。

图6-6

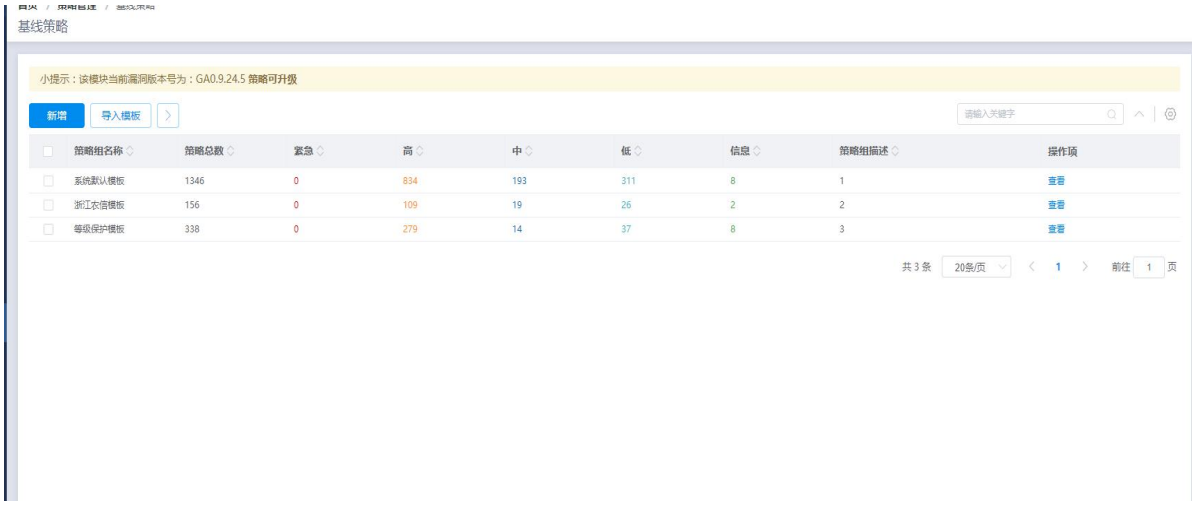
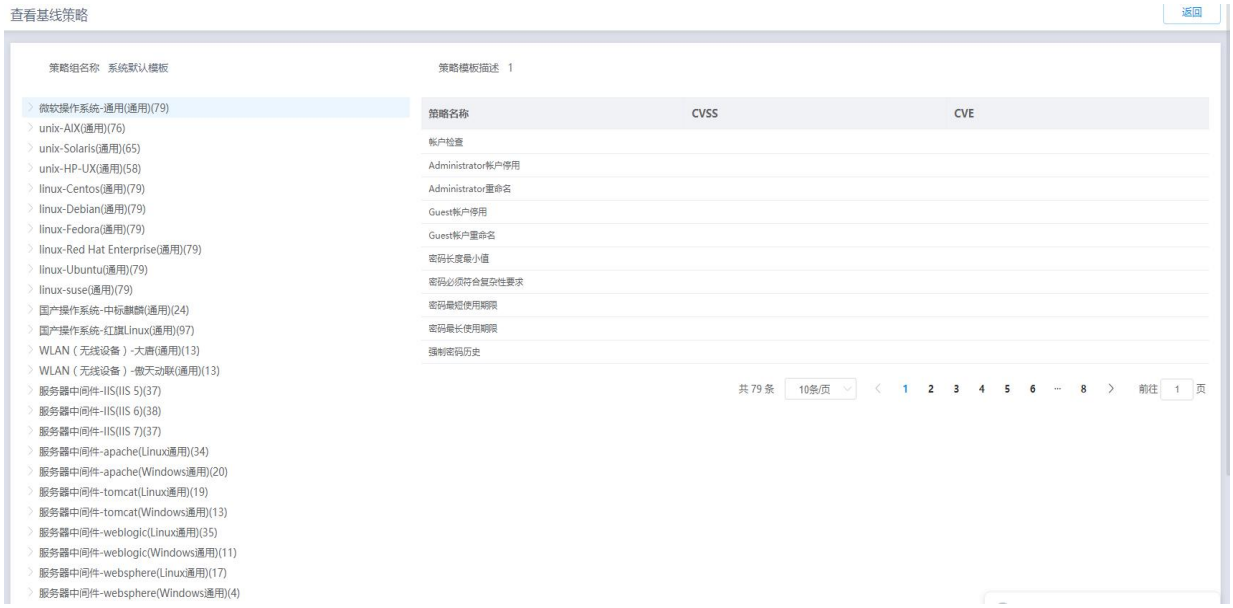


图 6-6 基线策略分组显示

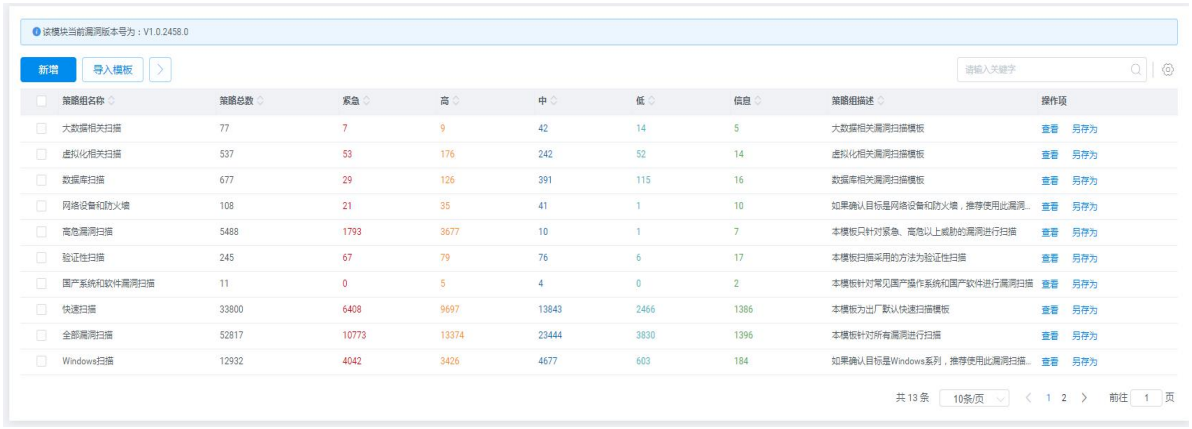
系统默认模板的查看 图6-7



6.4 主机策略

操作员用户根据已有的主机策略，创建策略分组，在新建主机扫描任务时，可以选择策略组进行主机扫描。点击【策略策略】→【主机策略】，如图 6-8所示。点击不同的类型，在右侧列表中显示不同的策略分组。

图6-8



查看各分组的策略内容可点击查看进行查看，如图6-9

图6-9

7 扫描任务

7.1 网站扫描

点击【扫描任务】→【网站扫描】→【新建】，打开网站扫描任务创建页面，如图 7-1 所示。

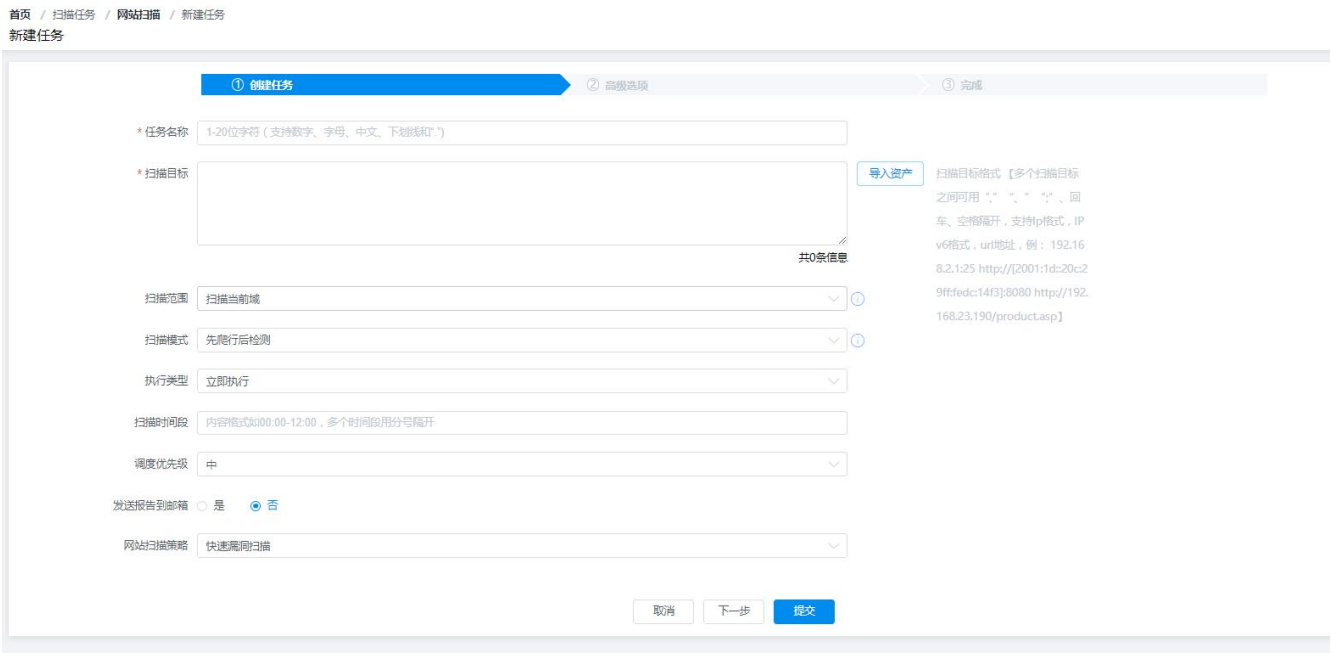


图 7-1 创建网站扫描任务

创建网站扫描任务填写信息输入项说明见下表 7-1。

表 7-1 创建网站扫描任务填写信息输入项说明

序号	输入项	说明	是否必填
1	任务名称	1-20位字符（支持数字/字母/中文/下划线/'.'）	是
2	扫描目标	格式：url地址，不得大于500个扫描目标，以回车结算。	是
3	扫描范围	支持扫描当前域、当前页、子路径、整个域、全部页，默认当前域，建议慎重使用全部页；	否
4	执行类型	支持手动执行，定时执行和周期执行，默认手动执行。	是
5	调度优先级	可设置高/中/低三种优先级。	是
6	是否发送报告到邮箱	默认选择否。若选择是，则需填写收件箱和邮件标题。	是
7	扫描时间段	可设置在某个时间段进行扫描；格式如00:00-12:00，多个时间段用分号隔开；	否
8	扫描模式	可以选择先爬行后检测、边爬行边检测、只检测、只爬行，默认先爬行后检测，默认即可；	否

9	网站扫描策略	可选择特定所需的扫描策略。	是
10	高级选项	包括扫描范围和扫描方式等。	否

填写好信息后，点击【提交】，完成网站扫描任务的创建。

任务创建成功后，显示在任务列表中，如图 7-2 所示

图 7-2 任务所示

可配置网站扫描过程中一些具体参数配置如图7-3

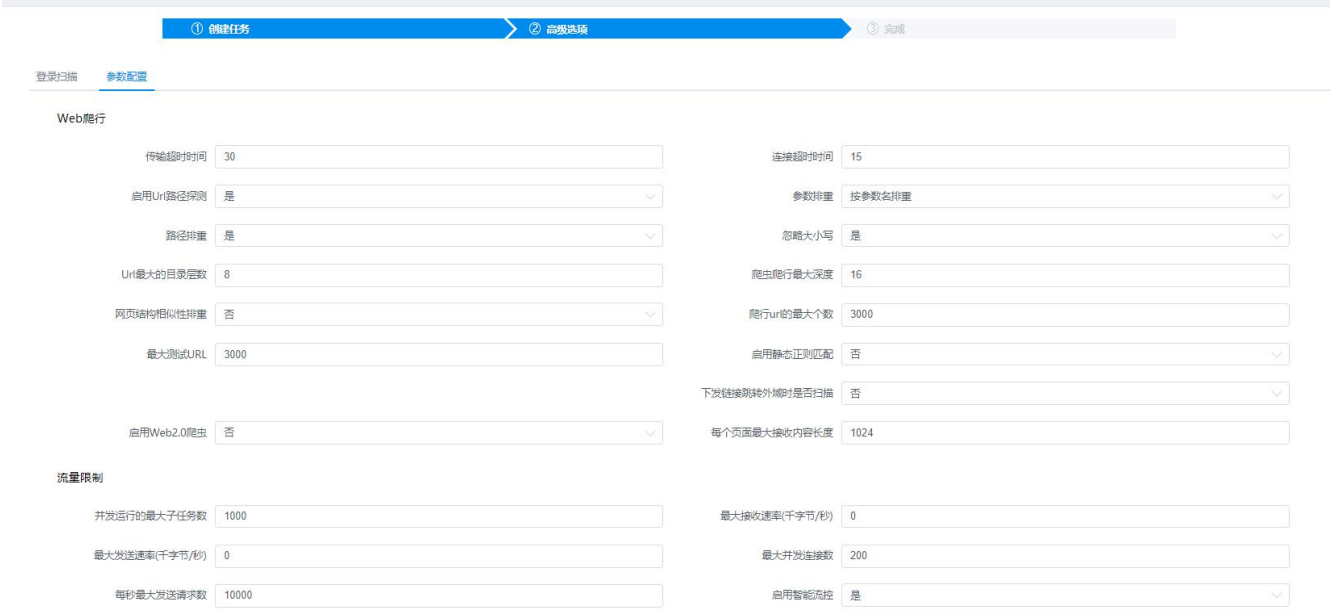


图7-3

点击任务列表中的删除，删除该任务。

点击任务列表中的停止，可停止扫描该任务。

点击任务列表中的暂停，可暂停扫描该任务。

点击任务列表的小齿轮  ，可自定义显示的列表项。

点击任务列表中的查看，可查看网站扫描结果，如图 7-4所示

图 7-4 网站任务扫描结果

在网站任务列表中可以根据网站状态、网站名称和网站地址进行查询相应网站。 点击网站扫描结果的详情，可查看到网站扫描状态和信息、漏洞信息和网站结构。网站扫描状态和信息，如图 7-5 所示 漏洞信息，如图 7-6 所示 网站结构，如图 7-7 所示

图 7-5 网站扫描状态和信息

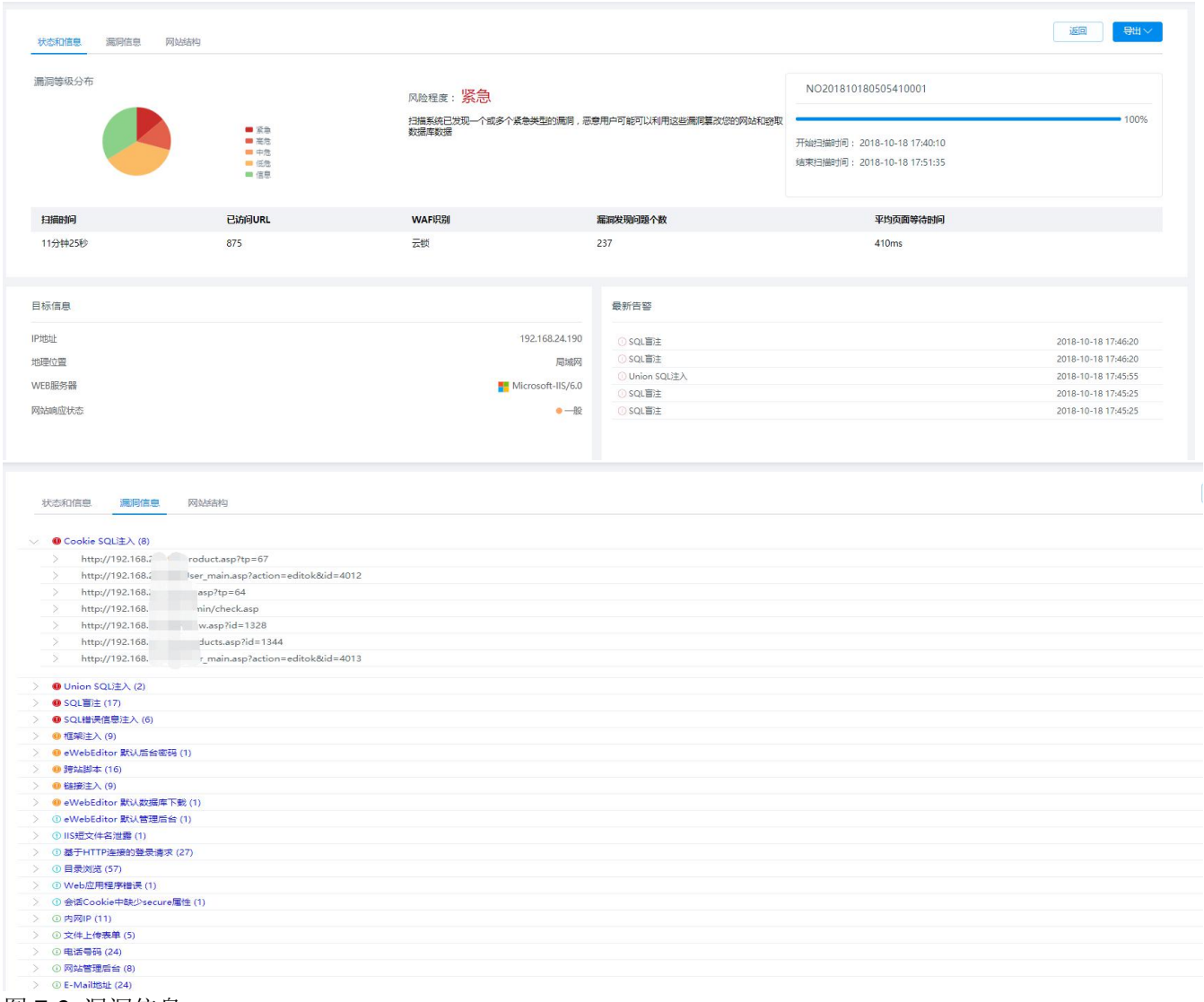


图 7-6 漏洞信息

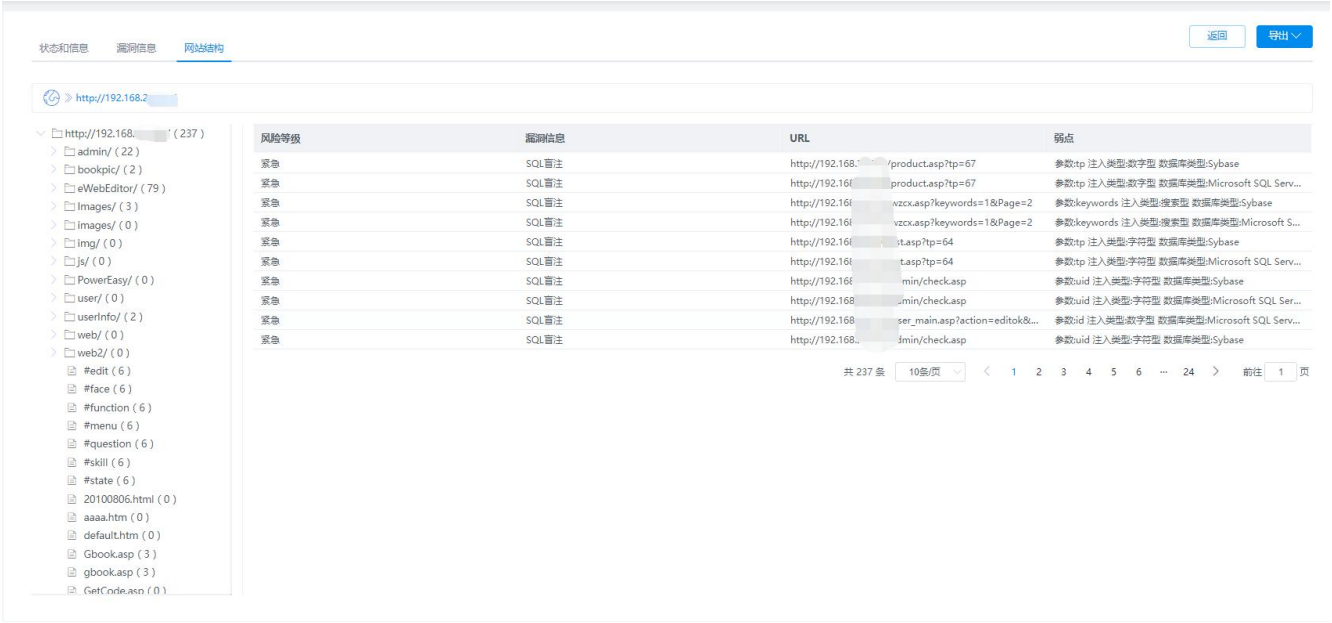
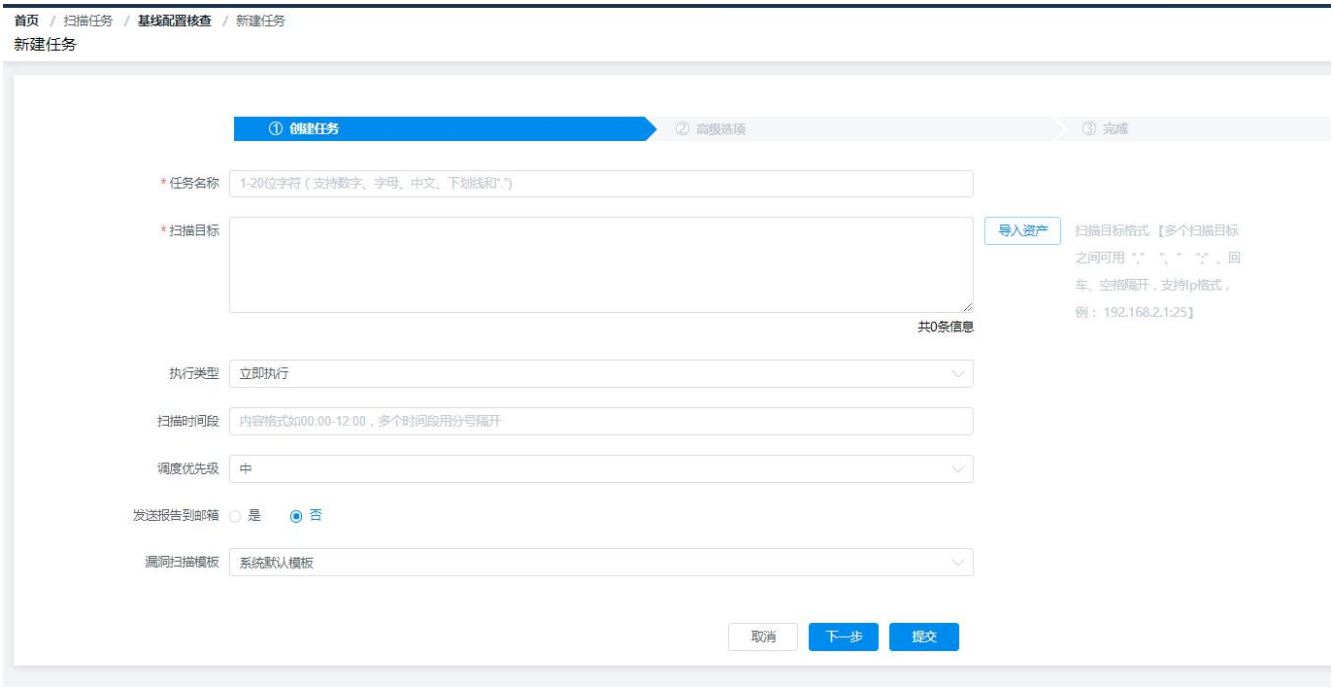


图7-7 网站结构图

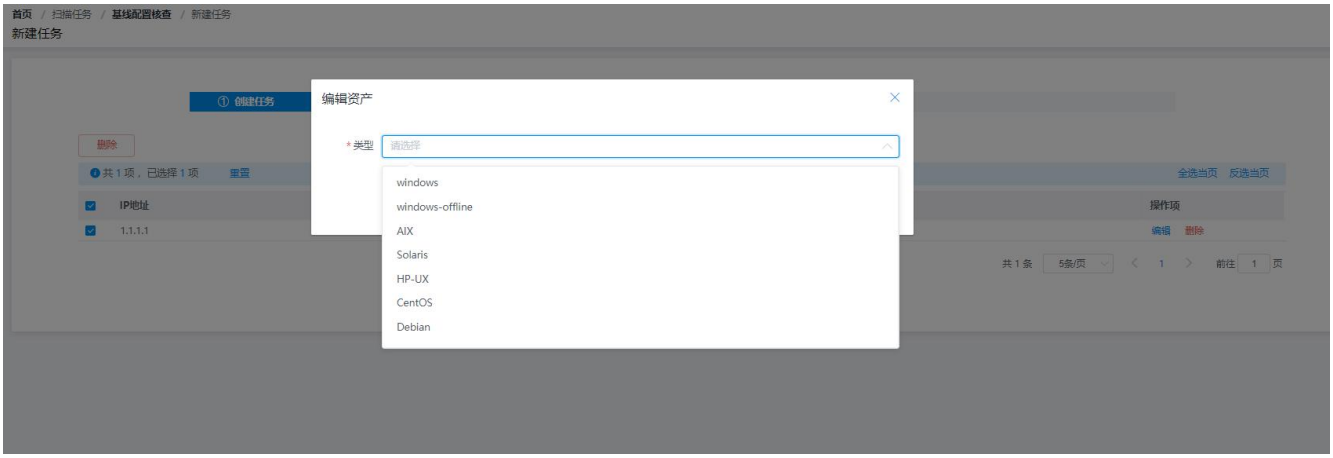
7.2 基线配置核查

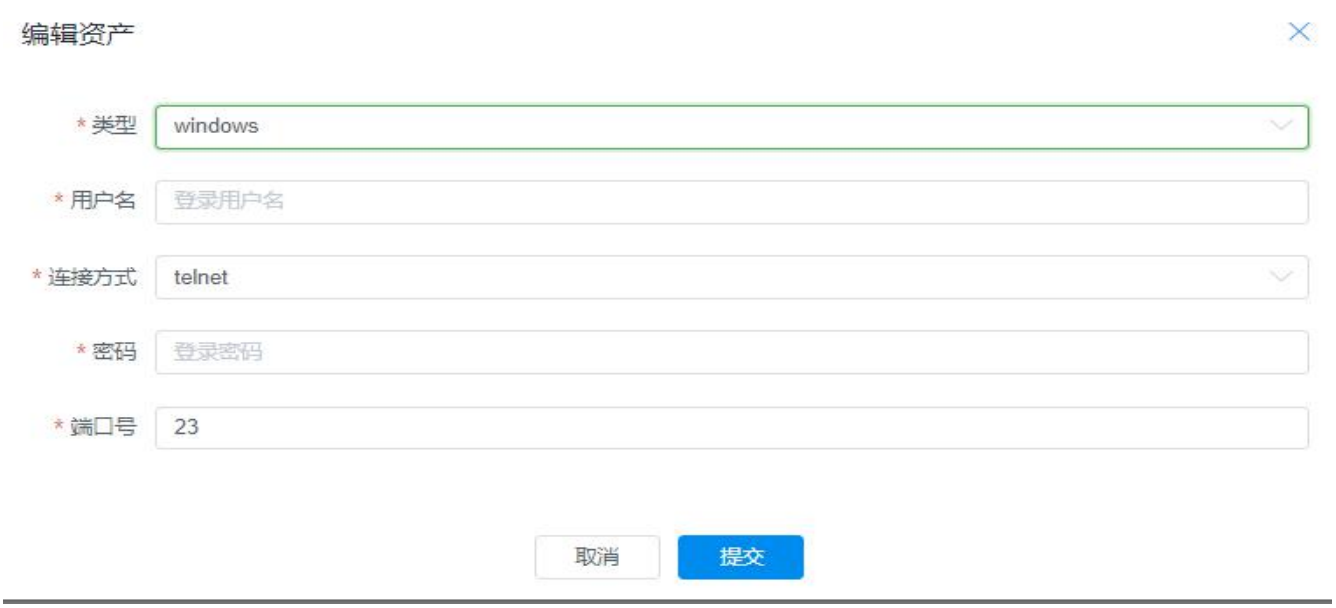
点击【扫描任务】→【基线配置核查】→【新增任务】，打开基线配置核查任务创建页面，如图 7-8 所示。

图 7-8 创建基线配置核查任务



需要下一步针对资产进行编辑选择登录的类型以及账户密码；





填写好信息后，点击【提交】完成基线配置核查任务的创建。

任务创建成功后，显示在任务列表中，如图 7-9所示

图7-9

点击任务列表中的执行，开始扫描任务。点击任务列表中的编辑，编辑任务信息。点击任务列表中的删除，删除该任务。

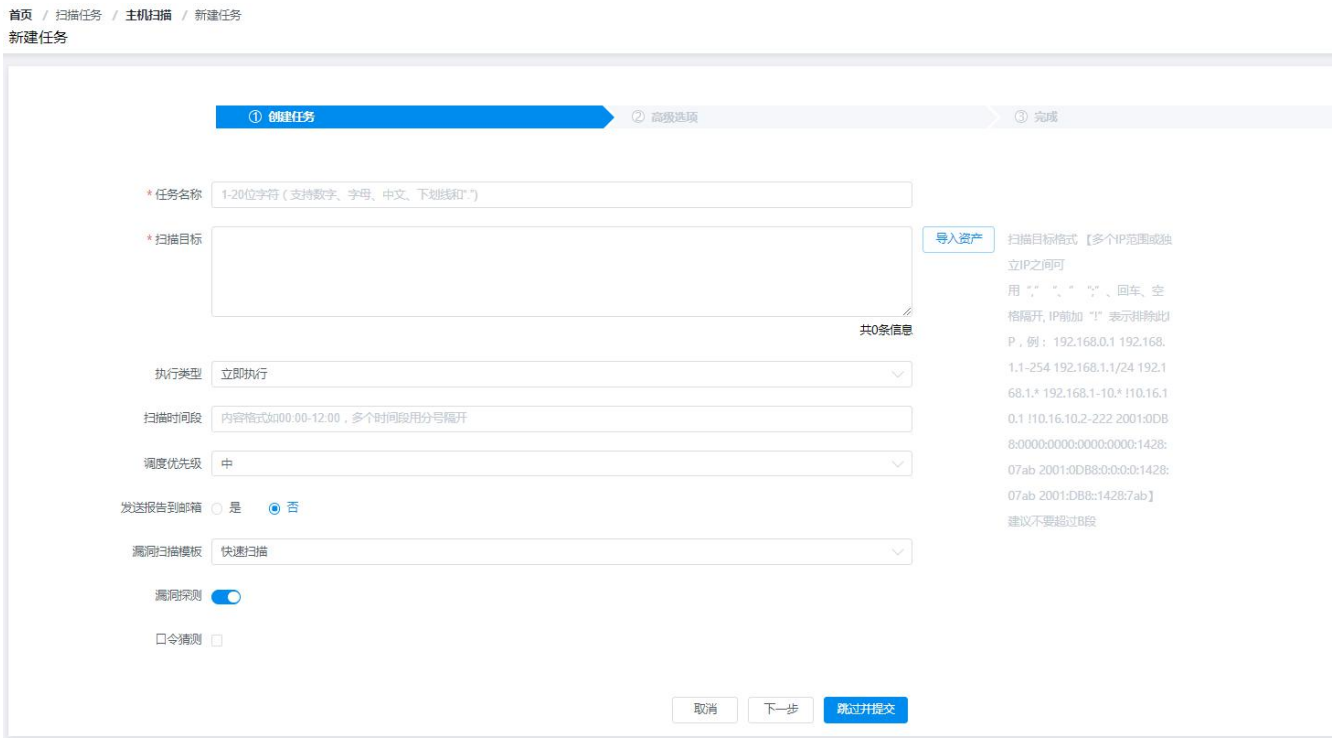
点击任务列表中的停止，可停止扫描该任务。

点击任务列表的小齿轮 ，可自定义显示的列表项。

7.3 主机扫描

点击【扫描任务】→【主机扫描】→【新增任务】，打开主机扫描任务创建页面，如图 7-10所示。

图 7-10 创建主机扫描任务



创建主机扫描任务填写信息输入项说明见下表 7-3。

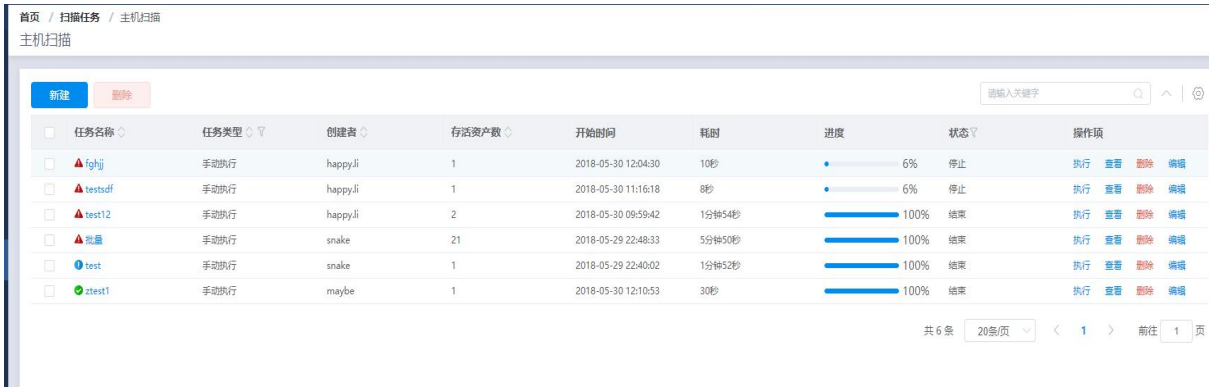
表 7-3 创建主机扫描任务填写信息输入项说明

序号	输入项	说明	是否必填
1	任务名称	1-20位字符（支持数字/字母/中文/下划线/'.'）	是
2	扫描目标	格式：IP，192.168.2.1:25，url地址，不得大于500个扫描目标，以回车结算。	否
3	执行类型	支持手动执行，定时执行和周期执行，默认手动执行。	是
4	调度优先级	可设置高/中/低三种优先级。	是
5	漏洞扫描模板	可选择扫描策略，内含快速扫描、完全扫描等	是
6	是否发送报告到邮箱	默认选择否。若选择是，则需填写收件箱和邮件标题。	是
7	网站扫描策略	可选择特定所需的扫描策略。	是
8	配置参数	下一步可以对各项高级参数进行配置。	否

填写好信息后，点击【提交】，完成网站主机任务的创建。

任务创建成功后，显示在任务列表中，如图 7-11 所示

图 7-11 任务所示



点击任务列表中的执行，开始扫描任务。

编辑任务可进行口令猜测编辑。

点击口令猜测的详细配置按钮，进行参数配置。如图 7-12 详细配置

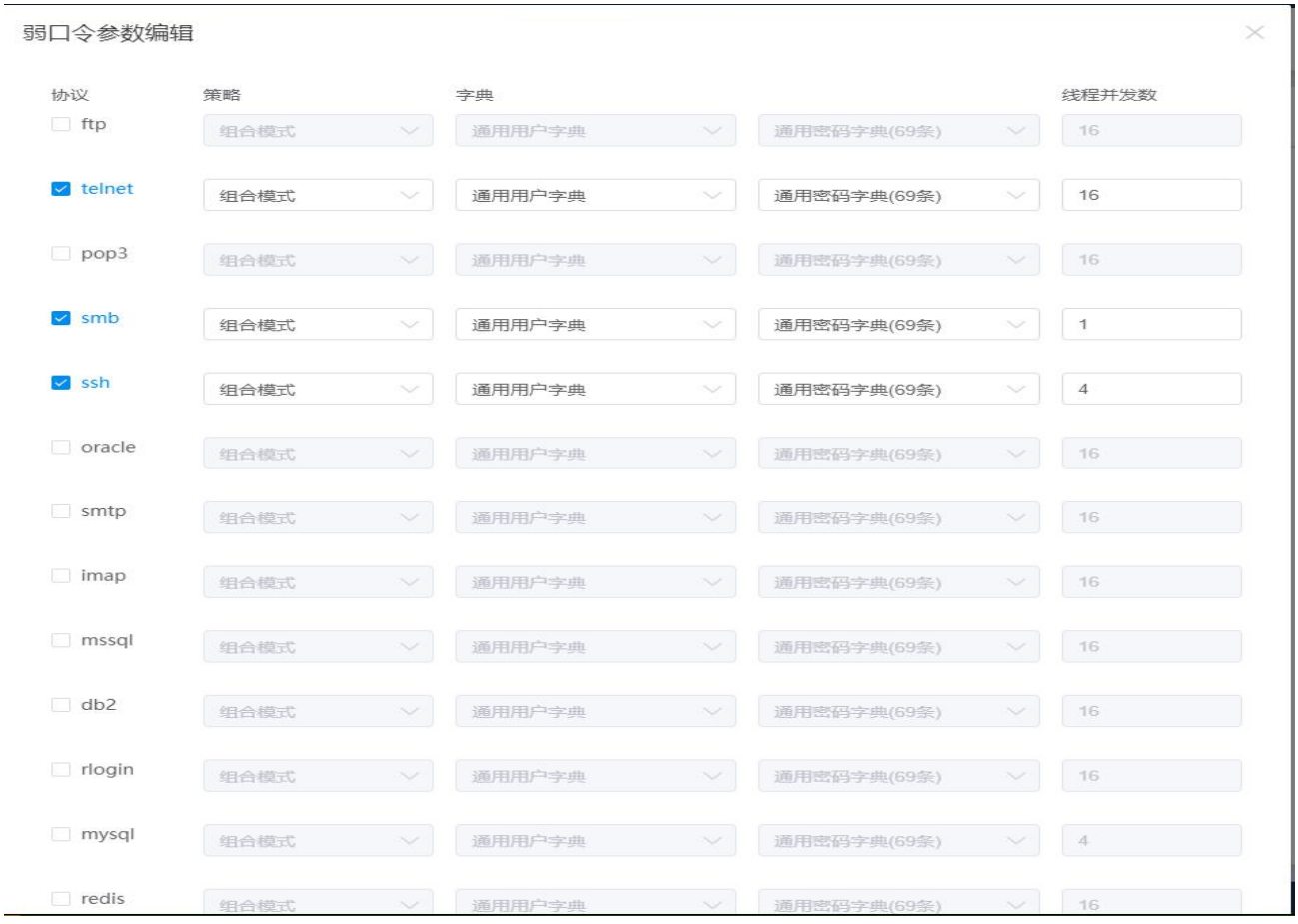
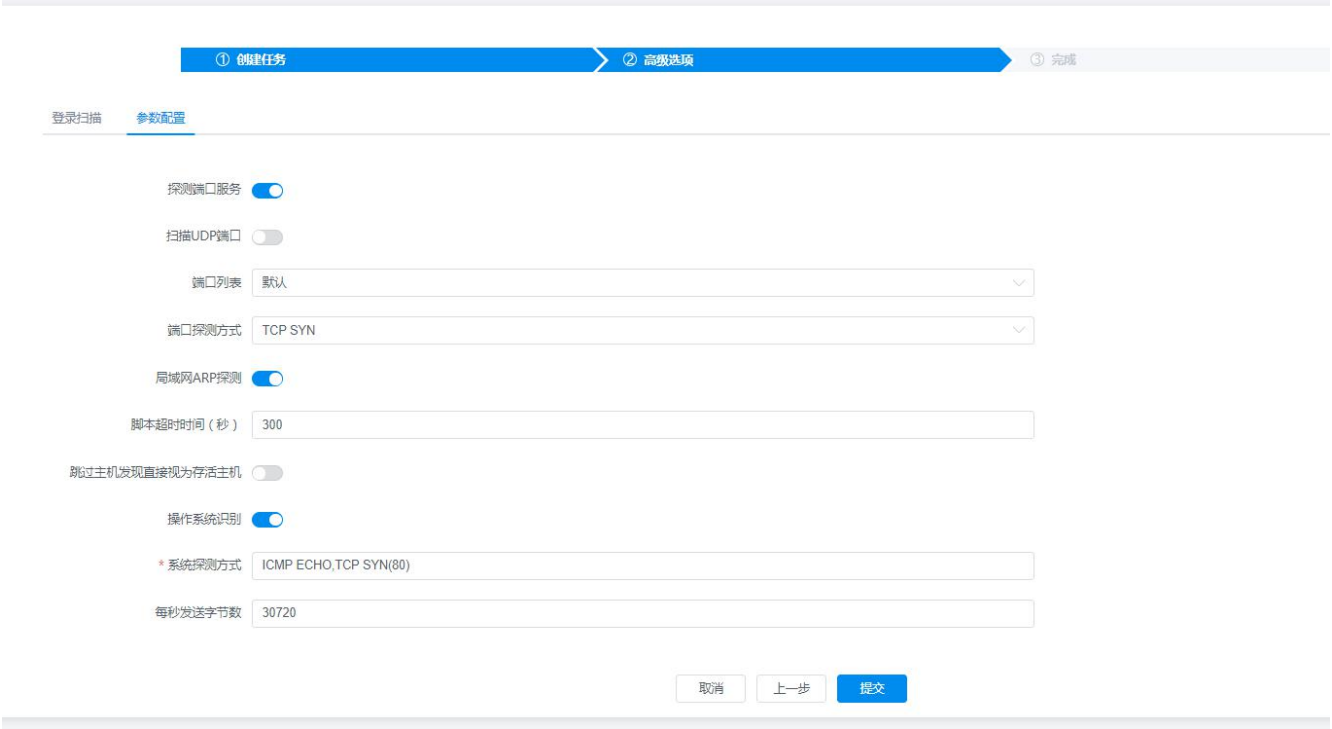


图 7-12 详细配置



点击任务列表中的删除，删除该任务。

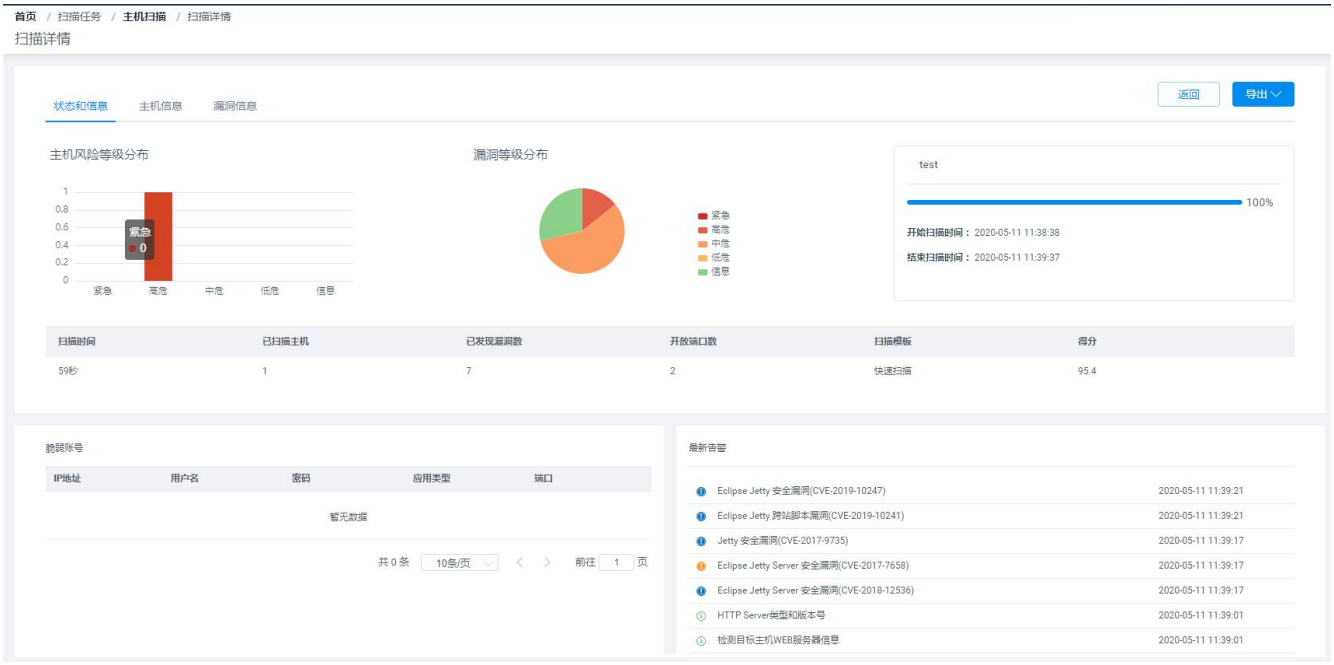
点击任务列表中的停止，可停止扫描该任务。

点击任务列表中的暂停，可暂停扫描该任务。

点击任务列表的小齿轮　　，可自定义显示的列表项。

点击任务列表中的任务名称，可查看主机扫描结果，如图 7-13 所示

图 7-13 主机任务扫描结果



点击查看主机信息可以查看到被扫描的主机信息,；点击漏洞信息可以查看到被扫描主机的漏洞分布。

主机信息，如图 7-14 所示　漏洞信息，如图 7-15 所示

图7-14主机信息

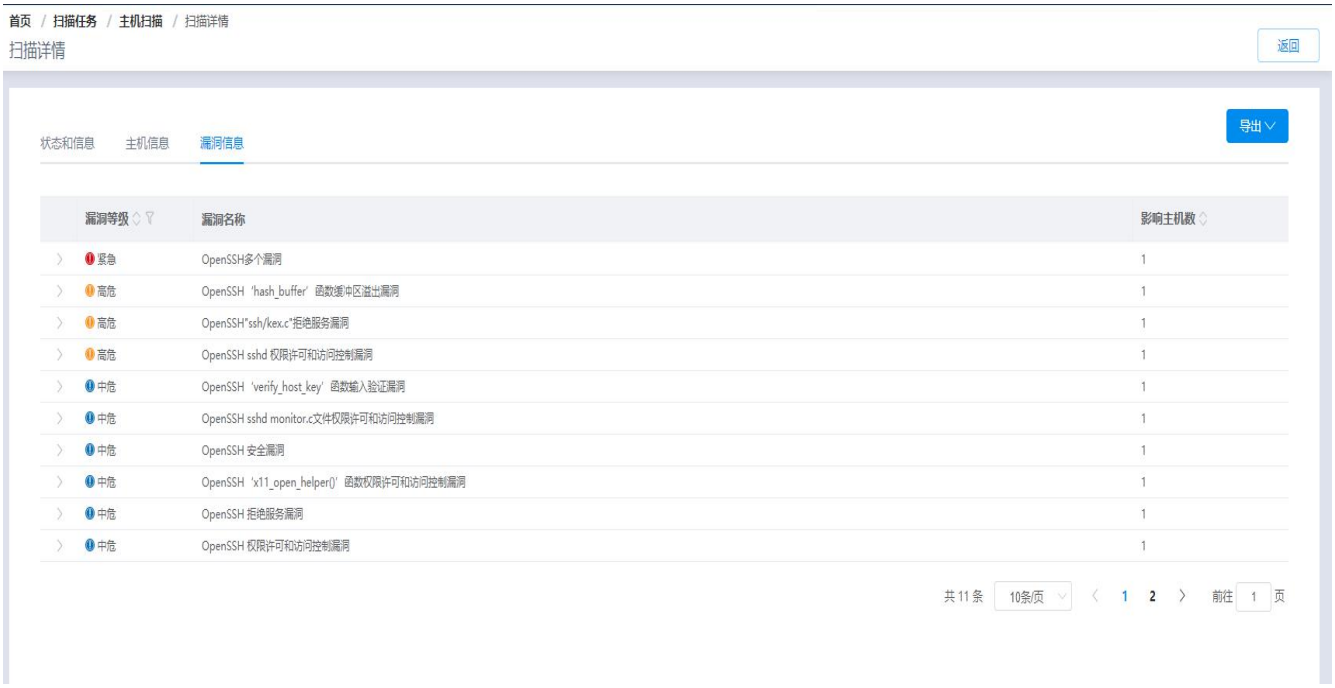
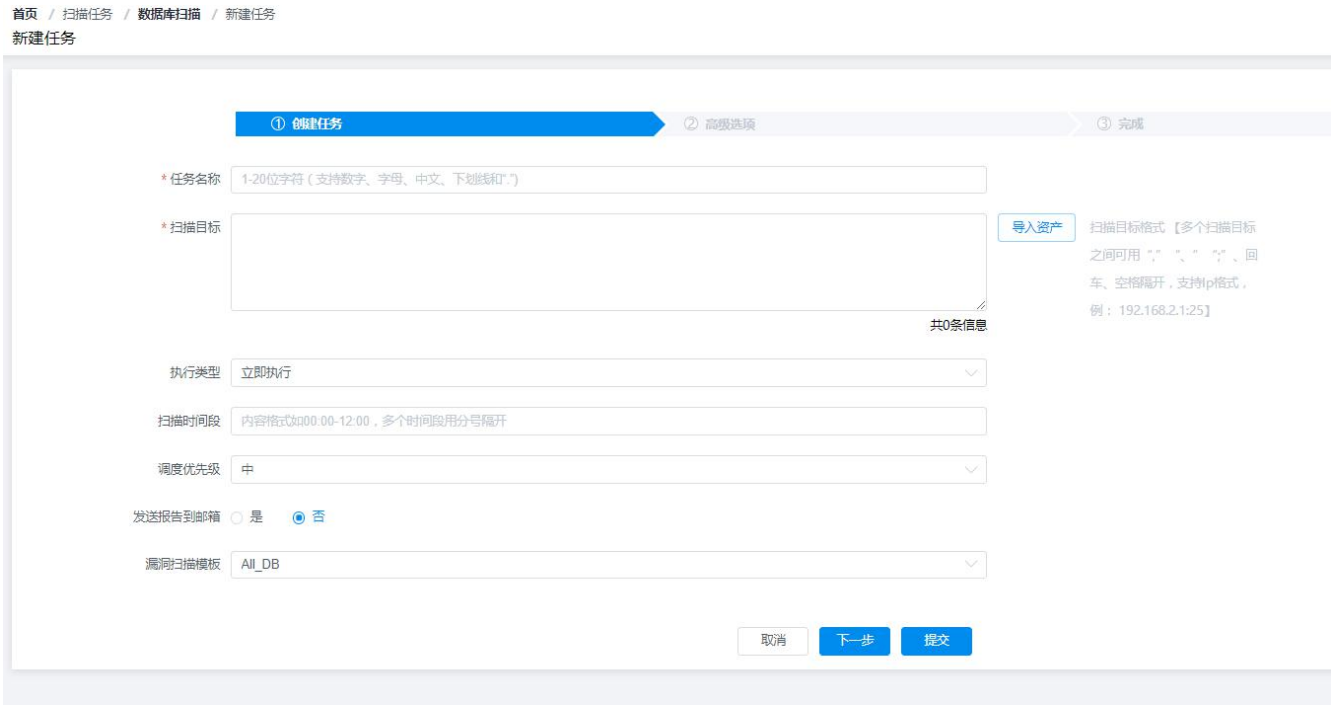


图7-15漏洞信息

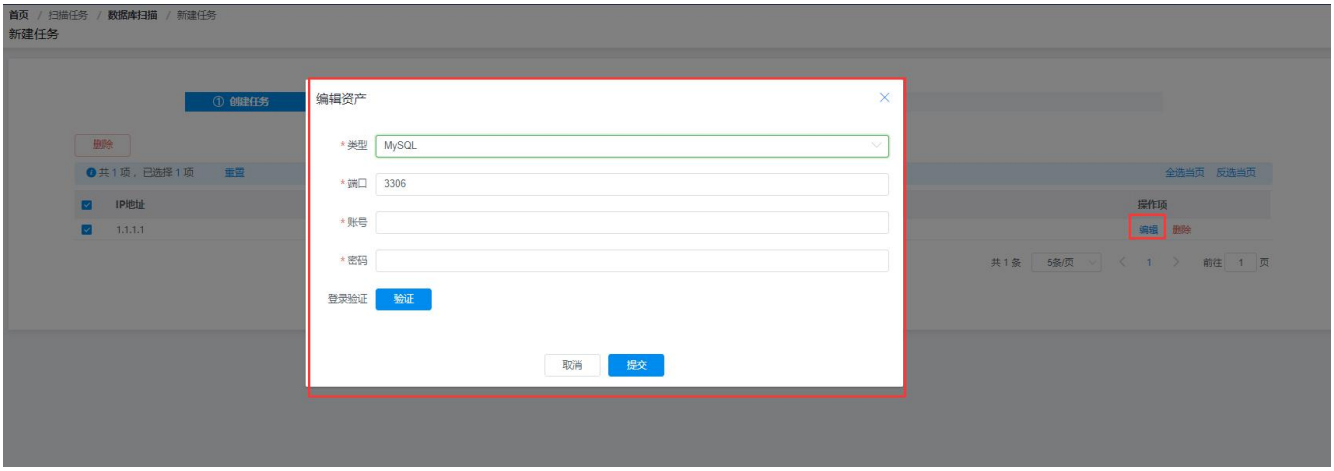
7.4 数据库扫描

点击【扫描任务】→【数据库扫描】→【新建】，打开数据库扫描任务创建页面，如图 7-16 所示。

图 7-16 创建数据库扫描任务



输入数据库地址后需要下一步编辑资产进行处理，



填写好信息后，点击【提交】完成升级扫描任务的创建。

点击任务列表中的删除，删除该任务。

任务创建成功后，显示在任务列表中，如图 7-17 所示

图 7-17 任务所示

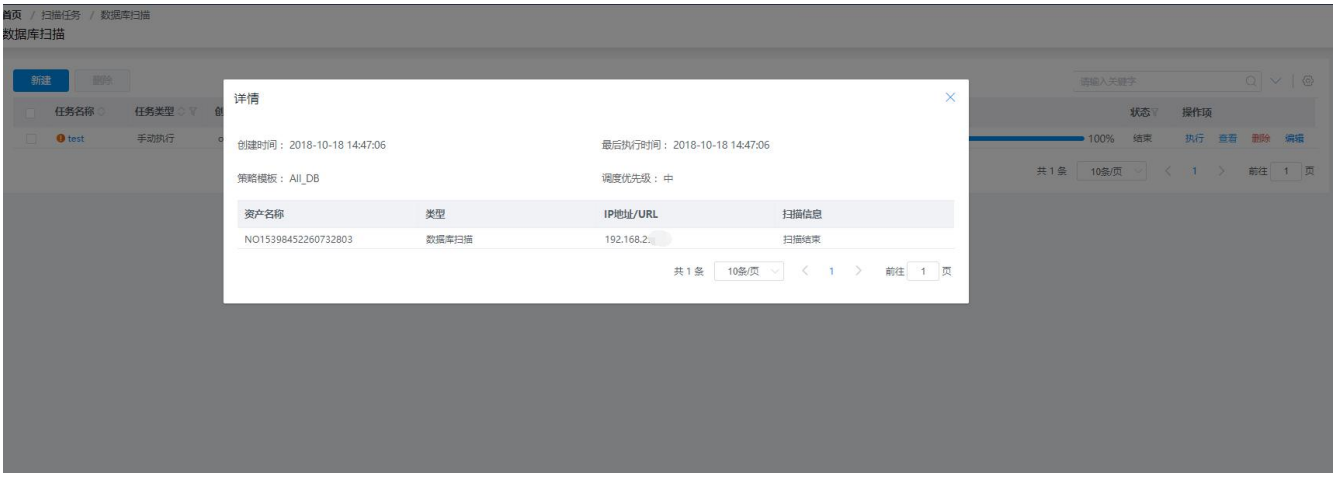
点击任务列表中的执行，开始扫描任务。

点击任务列表中的编辑，编辑任务信息。

点击任务列表中的删除，删除该任务。

点击任务列表中的查看，可查看数据库扫描信息，如图 7-18 所示

图 7-18 数据库扫描信息

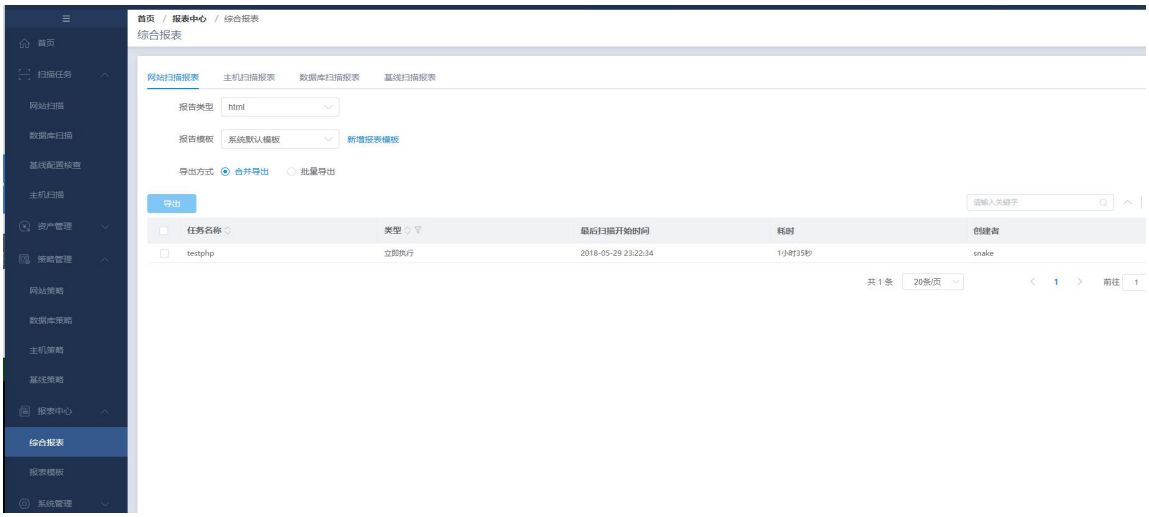


8 报告

8.1 综合报告

综合报告可显示所有扫描结束并且有扫描结果的任务，如图 8-1 所示。

图 8-1 综合报告



综合报表按照各个模块分别导出报告（包含：网站扫描报表、主机扫描报表、数据库扫描报表、基线扫描报表）；

可选择导出报告类型、导出报告模板、导出方式（合并导出和批量导出）；

以及可以选择对应的任务列表；

8.1.1 报表模板

可以预先设置所需报表，系统默认含有四个报表模板：系统默认模板、管理员模板、程序员模板、对比分析模板。如图 8-2 所示。

可以新建自定义报表模板；
可进行编辑标题、封面、logo、页眉、页脚、标题内容等相关信息；如图8-2

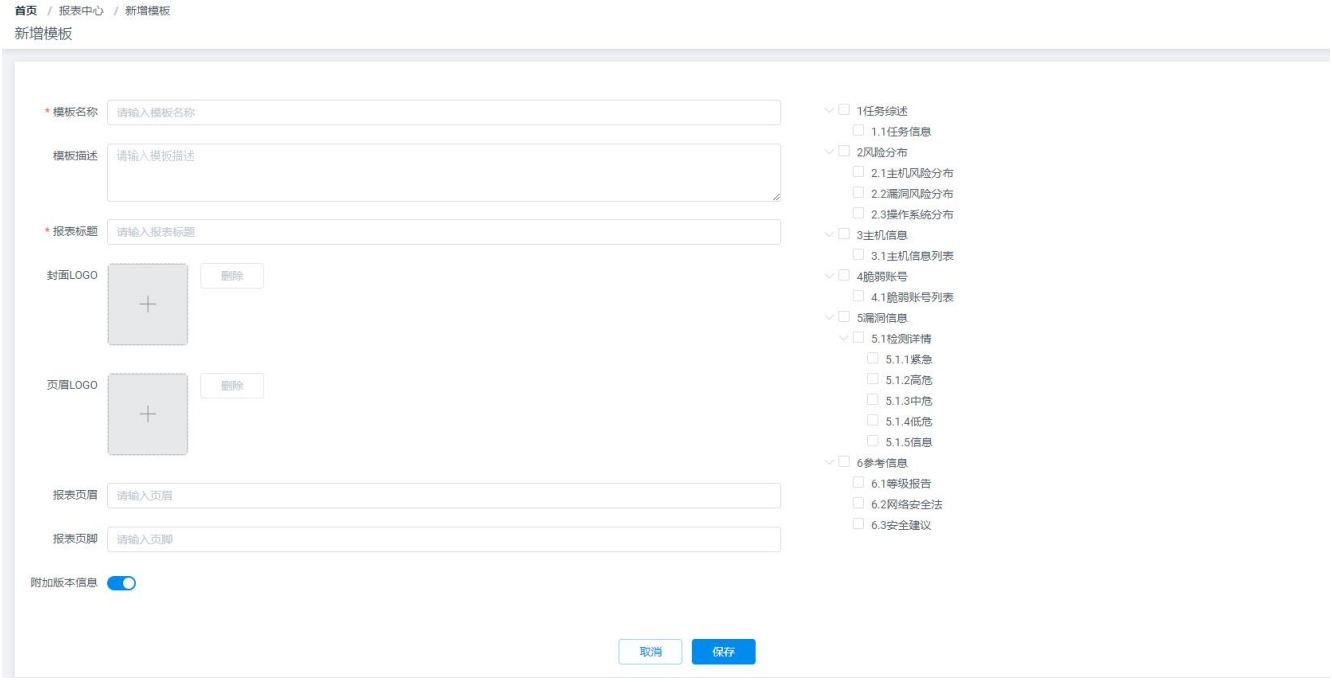


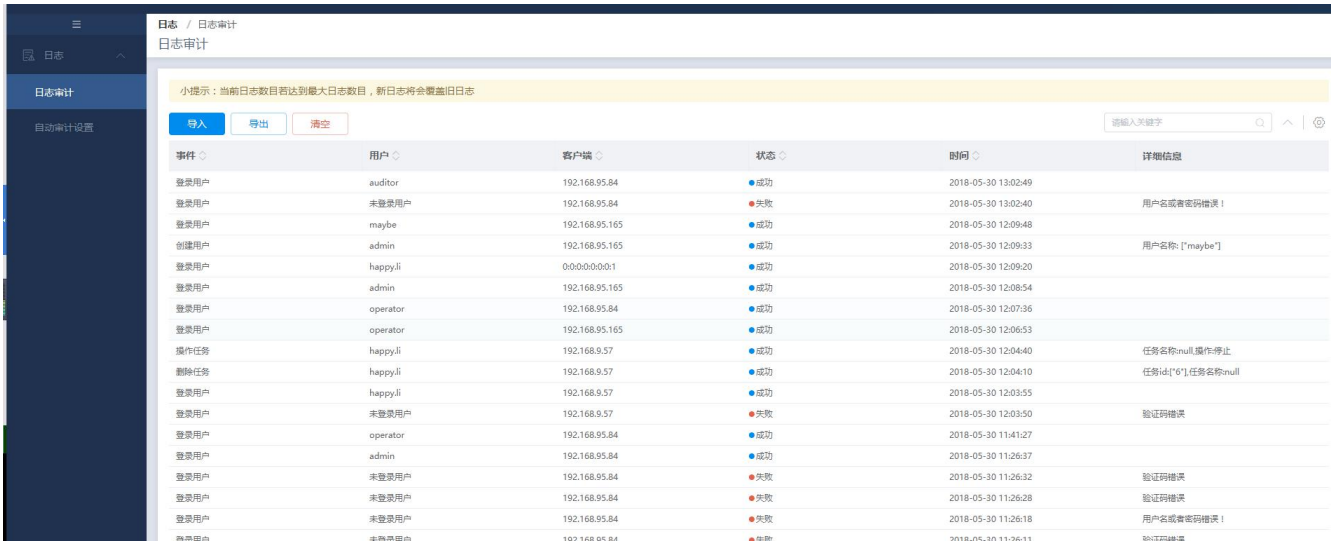
图8-3

9 日志

9.1 日志审计

日志审计是记录了所有用户的操作记录，包括事件名称、操作用户、操作客户端 IP 地址、事件状态、事件发生时间和事件详细信息，如下图 9-1 所示。

图 9-1 日志



点击上方的导出/导入可下载或上传日志内容，同时点击右上方的清空日志可一键清除所有记录的操作日志。

输入事件名称、操作用户、客户端操作 IP，选择状态和操作时间，可查询出符合条件的日志记录信息。

9.2 日志配置

9.2.1 备份方式

可以选择手动备份和自动备份功能，自动备份方式可以选择邮件备份和FTP备份方式，如图 9-2 所示。

9.2.2 阈值设置

日志配置可以设置阈值，如图 9-3 所示。

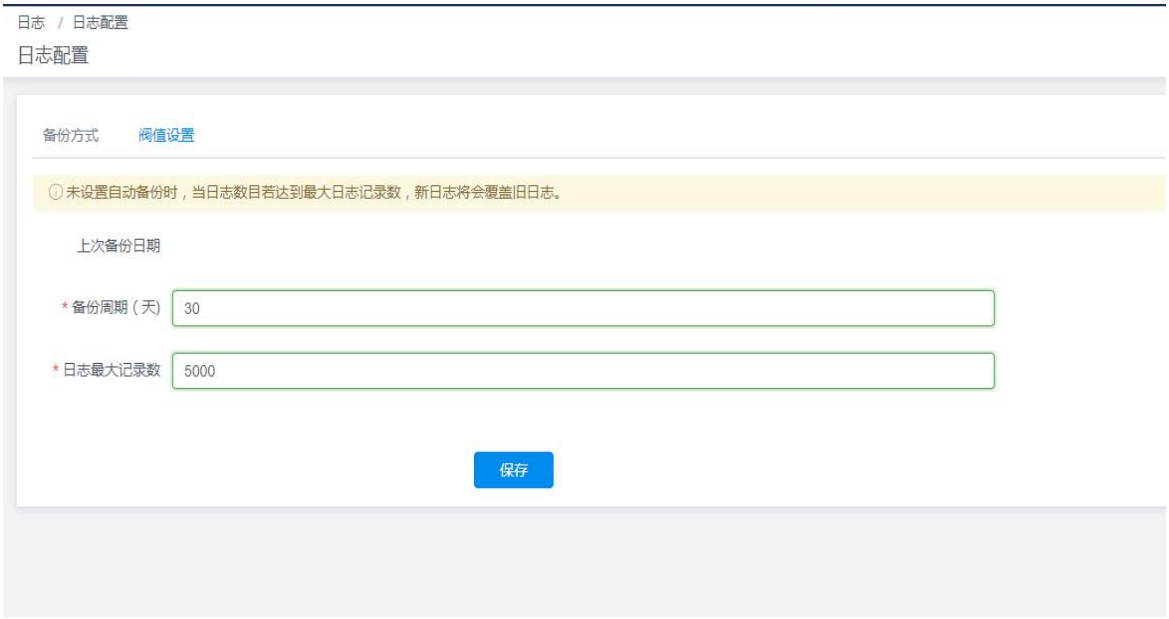


图 9-3 阈值设置

10 附录

10.1 网站资产配置参数详细说明

序号	分类	配置参数	详细说明
1	登录扫描	自定义User-Agent	指定用户代理，也就是产生当前请求的浏览器的类型，是HTTP请求头域中的组成部分。
2		Cookies	启动cookie录制，下载录制工具，执行程序，输入url即可获取对应cookie，填入文本框即可；
3		认证方式	默认设置无，可选择无、Basic、Diegest、自动（basic除外）、NTLM、Any和DigestIE。
4		域	对于域账户需要输入域名，没有可以不设置。
5		用户名	用于登录认证的用户名。

<table>
<tr><td>6</td><td rowspan="4"></td><td>密码</td><td>登录认证用户名对应的密码。</td></tr>
<tr><td>7</td><td>HTTPS双向认证的客户端证书</td><td>支持https证书上传，支持.crt,.cer,.cert,.key,.pem,.csr,.pfx,.der结尾格式的文件；</td></tr>
<tr><td>8</td><td>证书密码</td><td>证书文件的加密密码；</td></tr>
<tr><td>9</td><td>SSL版本</td><td>默认设置，支持SSLv2、SSLv3、TLSv1.X、TLSv1_0、TLSv1_1、TLSv1_2.;</td></tr>
<tr><td>10</td><td rowspan="5">参数配置/web爬行</td><td>传输时间</td><td>HTTP请求传输超时时间，单位秒</td></tr>
<tr><td>11</td><td>连接超时时间</td><td>HTTP请求建立连接超时时间，单位秒，应小于传输超时时间</td></tr>
<tr><td>12</td><td>启用URL路径探测</td><td>若启用则在扫描中爬行，主要针对ewebeditor，可以选择是/否，默认选择是。</td></tr>
<tr><td>13</td><td>参数排重</td><td>按参数名：对于多个参数相同，顺序不同，其它内容一致的URL，只爬行一次。
比如：随着爬行深入，出现了同参数名，顺序不同的URL链接，类似[http://192.168.23.5/web/product.asp?tp=67&a=3&b=4]的，只有tp、b、a参数的顺序不同，以下URL只爬行其中一个URL链接，其它链接不被扫描。
<table>
<tr><th></th><th>第一个参数</th><th>第二个参数</th><th>第三个参数</th></tr>
<tr><td>第1个URL</td><td>tp=67</td><td>a=31</td><td>b=4</td></tr>
<tr><td>第2个URL</td><td>tp=67</td><td>b=41</td><td>a=3</td></tr>
<tr><td>第3个URL</td><td>a=20</td><td>tp=67</td><td>b=55</td></tr>
<tr><td>第4个URL</td><td>a=35</td><td>b=4</td><td>tp=32</td></tr>
<tr><td>第5个URL</td><td>b=48</td><td>tp=65</td><td>a=34</td></tr>
<tr><td>第6个URL</td><td>b=40</td><td>a=3</td><td>tp=88</td></tr>
</table>
按参数组合：对于多个参数相同，顺序不同，其它内容一致的URL，将按照排列组合方式，扫描不同参数顺序的url链接。比如，以上例子中的url链接，总共包含3个不同参数tp、a、b，按照排列组合方法，即表中链接都被扫描。
无：表示所有的URL都进行爬行。
默认按参数名排重，可以选择无、按参数组合排重和按参数名排重。</td></tr>
<tr><td>14</td><td>路径排重</td><td>指对除数字之外其他内容一致的URL进行排重。即，假如2个URL的路径除了数字以外都一样的话，只有一个URL会被扫描，提高扫描效率。
比如，以下URL，若选择【路径模式排重】：“是”，会进行排重处理，最后只会扫描一个URL，下面的URL中只要扫到一个，其他的就不会进行扫描。
http://www.**.com/news/2010-12-02/1.html
http://www.**.com/news/2010-12-02/2.html
http://www.**.com/news/2010-12-03/1.html
http://www.**.com/news/2010-12-03/2.html
可以选择是/否，默认选择否。</td></tr>
<tr><td>15</td><td>忽略大小写</td><td>可以选择是/否，默认选择是。</td></tr>
</table>

16		Url最大的目录层数	目录层数是指URL的目录级数，每级目录为一个目录层数，一般以“/”进行分割，一个“/”为一级。 比如，http://192.168.23.190/cmssql/index.asp 里的cmssql为目录层数为1。默认设置8，设置为0时，表示没有层数限制。
17		爬虫爬行最大深度	设置爬行层数，控制扫描范围。 【深度--名词解释】：创建扫描任务会输入首个URL地址，引擎是从首个URL开始爬行。如从首个URL爬行到了A（URL）和B（URL），那么A和B相对于首个URL来说深度为1，从A又爬行到C（URL）和D（URL）。C和D相对首个URL来说深度为2。默认设置16，设置为0时，表示没有深度限制。
18		网页结构相似性排重	
19		爬行url的最大个数	根据页面内容结构相似度排重
20		最大测试URL	爬行最多发现的URL数量
21		启用静态正则匹配	发现的可进行测试的URL的最大个数
22		下发链接跳转外域时是否扫描	是否开启通过正则匹配查找网页中的URL
23		启用Web2.0爬虫	任务下发的url存在302跳转为限定域外的地址时是否进行扫描
24		每个页面最大接收内容长度	是否开启网页动态爬虫功能
25	流量限制	并发运行的最大子任务数	限制请求返回内容的最大长度，单位KB
26		最大接收速率(千字节/秒)	表示引擎最大接收速率，默认设置0，表示不限制。
27		最大发送速率(千字节/秒)	表示引擎最大发送速率，默认设置0，表示不限制。
28		最大并发连接数	表示引擎最大同时发送请求数，默认设置200
29		每秒最大发送请求数	表示引擎每秒最大发送请求个数，默认设置10000
30		启用智能流控	可以选择是/否，默认选择是。
31	表单	自动填充表单	用户可自定义字段和字段值，一旦扫描过程，此字段信息被匹配，就以自定义字段信息进行扫描。 比如：在自动填充表单详细配置列表中，添加个人的城市名，设置*city*=shanghai，当检测表单匹配到有包含city字符字段参数时，则用shanghai字段内容扫描，否则用默认数据进行设置扫描。默认“*addr*=newroad,*age*=24,*area*=021,*city*=newcity,*company*=mycom,*country*=china,*mail*=abc123@mycom.com,*day*=01,*month*=01,*year*=2011,*hour*=01,*num*=9876543210,*passport*=9876543210,*phone*=54321678,*tel*=54321678,*zip*=200085,*postal*=200085,*mobile*=13812345678,*code*=5431,*=1”。
32		初始的soap默认参数值	扫描webserver站点参数的默认值，类似于post表单的默认值。
33	Web检测	对匹配的Cookie字段在扫描时不做修改	对设置的字段不做修改。例如：cookie注入 会对cookie参数修改，但是某些参数例如sessionid如果修改了会导致登陆失

			败，需要设置对匹配的cookie字段在扫描时不做修改。 默认设置： *phpsessid*,*session*,*security*,*token*,*customcookie*,*engineid*,*formcerd*,*__utm*,*wt_fpc*,*__viewstate*,*__eventvalidation*,*__eventtarget*,*__eventargument*,*__previouspage*,*error*
34		尝试伪静态站点检测	是否把URL目录当成参数进行检测
35		Rewrite格式正则替换规则	对rewrite格式的URL进行正则替换； URL rewrite：服务器对URL解析的特殊规则 格式为：正则表达式1\n替换为的内容1\n正则表达式2\n替换为的内容2
36		忽略含有特殊关键字的链接	在检测的过程中，忽略含有特殊关键字的链接。当一个网页中的链接标签（比如html中的<a>标签，或者wap网页中的<go>标签）中含有该列表中的关键字时，就不对该链接进行爬行、检测。通常应该把那些会修改后台重要数据、会导致会话失效的链接的关键字加入该列表。用户可以根据需要自行设置参数值 默认设置：删,移除,停止,清空,注销,退出,再见,清除,重启,重载,无效,delete,remove,stop,undeploy,reload,restart,logout,signout,logoff,signoff,exit,quit,byebye,bye-bye,clearuser,invalidate。
37		不扫描的页面	检测网站过程中，对添加到该列表中的页面不执行扫描。添加到列表中的参数支持通配符。此选项也可以设置不爬行的目录，如以下URL http://www.a.com/dic/1.html，不想扫描dic目录，可以在此设置项添加*/dic/*，则URL里包含/dic/都不会被扫描。默认设置： */delete*,*logout*,*loginout*,*signout*,*logoff*,*signoff*,*exit*,*quit*,*byebye*,*bye-bye*,*clearuser*,*invalidate*,*security.php*,*reboot*,*shutdown*
38		不测试的文件后缀	对指定后缀的URL文件不进行测试，使用逗号分隔
39		有参数测试的文件后缀	对特定文件类型，若有请求参数则一定进行测试，使用逗号分隔
40	代理设置	代理类型	默认设置无，可以选择HTTP1.0、Socks4、HTTP、Socks4a和Socks5。
41		代理的IP地址和端口(IP:Port)	设置代理服务器地址和端口。
42		代理认证用户名	设置代理认证的用户名。
43		代理认证密码	设置代理认证的密码。

10.2数据库资产配置参数详细说明

序号	数据库类型	配置参数	详细说明	是否必填
1	Oracle	端口	Oracle数据库监听服务程序工作的端口，支持1-65535间数字	是
		实例名	Oracle数据库实例的服务名或SID实例名，该输入项与SID或Service_name选项设置关联	是

		SID	指定输入的实例名是数据库的服务名或SID实例名	是
		账号	设置连接数据库的用户名称	是
		密码	设置连接数据库所使用的用户的密码	是
2	SQL Server 2000	端口	数据库服务工作的端口，支持1-65535间数字	是
		账号	设置连接数据库的用户名称	是
		密码	设置连接数据库所使用的用户的密码	是
3	SQL Server 2005/2008	端口	数据库服务工作的端口，支持1-65535间数字	是
		账号	设置连接数据库的用户名称	是
		密码	设置连接数据库所使用的用户的密码	是
4	MySQL	端口	数据库服务工作的端口，支持1-65535间数字	是
		账号	设置连接数据库的用户名称	是
		密码	设置连接数据库所使用的用户的密码	是
5	DB2	端口	数据库服务工作的端口，支持1-65535间数字	是
		数据库名	设置要连接的数据库名称	是
		账号	设置连接数据库的用户名称	是
		密码	设置连接数据库所使用的用户的密码	是
6	Sybase	端口	数据库服务工作的端口，支持1-65535间数字	是
		账号	设置连接数据库的用户名称	是
		密码	设置连接数据库所使用的用户的密码	是
7	Informix	端口	数据库服务工作的端口，支持1-65535间数字	是
		服务名	设置要连接的数据库服务名称	是
		账号	设置连接数据库的用户名称	是
		密码	设置连接数据库所使用的用户的密码	是
8	DaMeng	端口	数据库服务工作的端口，支持1-65535间数字	是
		账号	设置连接数据库的用户名称	是
		密码	设置连接数据库所使用的用户的密码	是
9	Kingbase	端口	数据库服务工作的端口，支持1-65535间数字	是
		账号	设置连接数据库的用户名称	是
		密码	设置连接数据库所使用的用户的密码	是

10.3主机资产配置参数详细说明

序号	分类	配置说明
1	端口探测服务	默认开启，扫描操作系统端口服务.

2	扫描UDP端口	默认选择否。启用后会探测UDP端口.
3	端口列表	有默认值，也可以自行选择，或者自定义端口扫描.
4	端口探测方式	默认TCP SYN.
5	局域网ARP探测	默认开启。启用后ARP地址解析协议去探测主机，使探测主机更准确
6	脚本超时时间	单条策略超时时间，单位秒，默认300秒；
7	跳过主机发现直接视为存活主机	默认关闭，启用服务即直接将扫描主机视为存活进行端口探测；
8	操作系统识别	默认开启，识别主机操作系统版本；
9	系统探测方式	默认ICMP ECHO,TCP SYN(80)，如主机禁ping，可设置TCP SYN(80)；
10	每秒发送字节数	用于调节扫描速率，默认30720。可设定范围0-10485760；

10.4基线资产配置参数详细说明

序号	分类	配置参数	详细说明
1	windows	扫描方式/其他	默认为远程扫描，当选择其他时，须上传报告文件。
		端口号	默认端口为23。
		用户名	设置连接基线的用户名。
		密码	设置连接基线的密码。
		连接方式	可选择默认的telnet或smb连接。
2	AIX、Solaris、HP-UX、CentOS、Debian、Fedora、RedHat、Ubuntu、SUSE、中标麒麟、红旗、大唐、傲天动联、VMWare Esxi5/6	端口号	默认端口为22。
		用户名	设置连接基线的用户名。
		密码	设置连接基线的密码。
		管理员密码	设置管理员密码。
		连接方式	可选择默认的telnet或smb连接。
3	IIS5、IIS6、IIS7、Apache Windows、Tomcat Windows、Weblogic Windows、Websphere Windows、Jboss4 Windows、Jboss5 Windows、Jboss6 Windows、Resin Windows、Nginx Windows	报告文件	需从本地上传文件。
4	Apache Linux、TomcatLinux、TongWeb、Resin Linux 、Nginx Linux 、Bind Linux	端口号	默认端口为22。
		用户名	设置系统用户名。
		密码	设置系统密码。
		管理员密码	设置管理员密码。
		连接方式	可选择默认的telnet或smb连接。
		配置文件目录	设置默认的配置文件目录。
5	Weblogic Linux	端口号	默认端口为22。

		用户名	设置系统用户名。
		密码	设置系统密码。
		管理员密码	设置管理员密码。
		连接方式	可选择默认的telnet或smb连接。
		域路径	设置域所在的路径。
		服务名称	设置服务名称，例如server1。
6	Websphere Linux	端口号	默认端口为22。
		用户名	设置系统用户名。
		密码	设置系统密码。
		管理员密码	设置管理员密码。
		连接方式	可选择默认的telnet或smb连接。
		根目录	输入软件安装的根目录。
		概要名称	Websphere概要名称，如AppSrc01。
		单元名称	设置单元名称。
		节点名称	设置节点名称。
		服务名称	设置服务名称。
7	Jboss4 Linux、Jboss5 Linux、Jboss6 Linux	端口号	默认端口为22。
		用户名	设置用户名。
		密码	设置系统密码。
		管理员密码	设置管理员密码。
		连接方式	可选择默认的telnet或smb连接。
		根目录	输入软件安装的根目录。
		服务名称	设置服务名称。

10.5弱口令资产配置参数详细说明

序号	分类	配置参数	详细说明
1	SMB	是否扫描此协议	是/否，默认选择否。smb协议是windows系统登录使用的协议。
		用户名字典	可选择默认字典或者用户自定义字典。
		密码字典	可选择默认字典或者用户自定义字典。
		端口号	默认445
		任务并发数	默认1。
		口令尝试次数	默认1。
		该协议找到一对可用弱口令后是否终止扫描	是/否，默认选择是。
2	TELNET	是否扫描此协议	是/否，默认选择否。Telnet协议是TCP/IP协议族中的一员，是Internet远程登陆服务的标准协议和主要方式。
		用户名字典	可选择默认字典或者用户自定义字典。
		密码字典	可选择默认字典或者用户自定义字典。
		端口号	默认23
		任务并发数	默认16
		口令尝试次数	默认1
		该协议找到一对可用弱口令后是否终止扫描	是/否，默认选择是。

3	FTP	是否扫描此协议	是/否，默认选择否。FTP（File Transfer Protocol，文件传输协议） 是 TCP/IP 协议组中的协议之一。FTP协议包括两个组成部分，其一为FTP服务器，其二为FTP客户端
		用户名字典	可选择默认字典或者用户自定义字典。
		密码字典	可选择默认字典或者用户自定义字典。
		端口号	默认23
		任务并发数	默认16
		口令尝试次数	默认1
		该协议找到一对可用弱口令后是否终止扫描	是/否，默认选择是。
4	RDP	是否扫描此协议	是/否，默认选择否。RDP，远程显示协议（Remote Display Protocol ）
		用户名字典	可选择默认字典或者用户自定义字典。
		密码字典	可选择默认字典或者用户自定义字典。
		端口号	默认3389
		任务并发数	默认4
		口令尝试次数	默认1
		该协议找到一对可用弱口令后是否终止扫描	是/否，默认选择是。
5	SSH	是否扫描此协议	是/否，默认选择否。Ssh协议是linux系统登录使用的协议。
		用户名字典	可选择默认字典或者用户自定义字典。
		密码字典	可选择默认字典或者用户自定义字典。
		端口号	默认22
		任务并发数	默认4
		口令尝试次数	默认1
		该协议找到一对可用弱口令后是否终止扫描	是/否，默认选择是。
6	POP3	是否扫描此协议	是/否，默认选择否。pop3协议主要用于支持使用客户端远程管理在服务器上的电子邮件。
		用户名字典	可选择默认字典或者用户自定义字典。
		密码字典	可选择默认字典或者用户自定义字典。
		端口号	默认110
		任务并发数	默认16
		口令尝试次数	默认1
		该协议找到一对可用弱口令后是否终止扫描	是/否，默认选择是。

7	IMAP	是否扫描此协议	是/否，默认选择否。Imap是交互邮件访问协议
		用户名字典	可选择默认字典或者用户自定义字典。
		密码字典	可选择默认字典或者用户自定义字典。
		端口号	默认143
		任务并发数	默认16
		口令尝试次数	默认1
		该协议找到一对可用弱口令后是否终止扫描	是/否，默认选择是。
8	SMTP	是否扫描此协议	是/否，默认选择否。Smtp是简单邮件传输协议
		用户名字典	可选择默认字典或者用户自定义字典。
		密码字典	可选择默认字典或者用户自定义字典。
		端口号	默认25
		任务并发数	默认16
		口令尝试次数	默认1
		该协议找到一对可用弱口令后是否终止扫描	是/否，默认选择是。
9	SQL SERVER	是否扫描此协议	是/否，默认选择否。Sql server协议是访问该数据库的协议
		用户名字典	可选择默认字典或者用户自定义字典。
		密码字典	可选择默认字典或者用户自定义字典。
		端口号	默认1433
		任务并发数	默认16
		口令尝试次数	默认1
		该协议找到一对可用弱口令后是否终止扫描	是/否，默认选择是。
10	MySQL	是否扫描此协议	是/否，默认选择否。Mysql协议是访问该数据库的协议
		用户名字典	可选择默认字典或者用户自定义字典。
		密码字典	可选择默认字典或者用户自定义字典。
		端口号	默认3306
		任务并发数	默认16
		口令尝试次数	默认4
		该协议找到一对可用弱口令后是否终止扫描	是/否，默认选择是。
11	Oracle	是否扫描此协议	是/否，默认选择否。Oracle协议是访问该数据库的协议
		用户名字典	可选择默认字典或者用户自定义字典。

		密码字典	可选择默认字典或者用户自定义字典。
		数据库名	默认orcl
		端口号	默认1521
		任务并发数	默认16
		口令尝试次数	默认4
		该协议找到一对可用弱口令后是否终止扫描	是/否，默认选择是。
12	DB2	是否扫描此协议	是/否，默认选择否。Db2协议是访问该数据库的协议
		用户名字典	可选择默认字典或者用户自定义字典。
		密码字典	可选择默认字典或者用户自定义字典。
		数据库名	默认sample
		端口号	默认50000
		任务并发数	默认16
		口令尝试次数	默认4
		该协议找到一对可用弱口令后是否终止扫描	是/否，默认选择是。
13	SNMP	是否扫描此协议	是/否，默认选择否。Snmp是简单网络管理协议
		密码字典	可选择默认字典或者用户自定义字典。
		端口号	默认161
		任务并发数	默认16
		口令尝试次数	默认4
		该协议找到一对可用弱口令后是否终止扫描	是/否，默认选择是。