UNIS XScan-G 系列漏洞扫描系统

Web 配置指导

北京紫光恒越网络科技有限公司
http://www.unishy.com

资料版本：5W100-20180415

前 言

本手册指导主要介绍 UNIS XScan-G 系列漏洞扫描系统 Web 页面上的配置内容。

前言部分包含如下内容：

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格　式	意　义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从多个选项中仅选取一个。
[x | y | ...]	表示从多个选项中选取一个或者不选。
{ x | y | ... } *	表示从多个选项中至少选取一个。
[x | y | ...] *	表示从多个选项中选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1～n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格　式	意　义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 端口编号示例约定

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

技术支持

用户支持邮箱：zgsm_service@thunis.com

技术支持热线电话：400-910-9998（手机、固话均可拨打）

网址：http://www.unishy.com

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：zgsm_info@thunis.com

感谢您的反馈，让我们做得更好！

目 录

1 概述

1.1 产品简介

UNIS 系统漏洞扫描系统是北京紫光恒越网络科技有限公司的安全团队在积累了多年安全研究成果和服务实践经验的基础上，自主研发的一款基于 B/S 架构，用于评估目标网络安全状态的综合漏洞扫描系统。该系统严格按照计算机信息系统安全的国家标准、相关行业标准设计、编写，拥有优秀底层核心引擎、全面的漏洞检测规则和领先的扫描技术，可对主流操作系统、Web 应用、数据库、网络设备、常见应用等目标进行深入扫描，发现可被黑客利用的安全漏洞、弱口令和其他脆弱性，并针对每一个安全问题提供详尽、专业、有效的安全建议和修补方案，协助安全人员把安全风险降到可接受范围内。

该系统支持主机漏洞扫描、Web 漏洞扫描和数据库漏洞扫描三大模块：

- 主机漏洞扫描模块，支持检测主流操作系统、网络设备、常见应用、数据库系统等对象。检测类型包含内存破坏类漏洞、CGI 类漏洞、输入验证类漏洞、配置错误类漏洞、系统本地补丁、常见协议弱口令、木马病毒等。
- Web 漏洞扫描模块，全面支持 OWASP TOP 10 检测。支持 SQL 注入攻击、跨站脚本、文件包含、远程代码执行、主流 CMS 漏洞检测等。
- 数据库扫描模块，支持以登陆方式检测主流数据库系统的弱密码和数据库安全漏洞。支持 Oracle、MySQL、SQL Server、DB2、Informix、Sybase、达梦等主流数据库数据库类型。

漏洞扫描系统可作为防火墙和入侵防御系统的补充，能够有效地降低网络安全管理员的工作量，准确高效地评估当前网络的安全状态，及时发现网络中存在的安全问题，合理解决或规避网络风险。广泛应用于政府、公安、教育、卫生、电力、金融等行业，帮助用户解决目前所面临的各类常见及最新的安全问题，同时满足如等级保护、行业规范等政策法规的安全建设要求。

1.2 图形界面格式约定

表1-1 图形界面格式预定表

格式	描述
【】	代表菜单或子菜单名称
>	代表Web网管配置路径：如【扫描】>【任务管理】，表示“扫描”菜单下的“任务管理”菜单
<>	代表窗口中的选项或按钮名称
	代表“其他配置”菜单名称
	代表“帮助”菜单名称
	用户头像

1.3 环境要求

设备系列产品可在如下环境使用：

- 输入电压：220～240V。
- 温度：-10～50°C。
- 湿度：5～90%。
- 电源：交流电源 110V～230V。

为保证系统能长期稳定的运行，应保证电源有良好的接地措施、防尘措施、保持使用环境的空气通畅和室温稳定。本产品符合关于环境保护方面的设计要求。

提示

- 保证设备工作在建议的环境要求内，否则可能导致设备损坏或提早老化。
- 设备良好的接地可以有效避免雷击。

1.4 接线方式

请按照如下步骤进行设备的接线：

(1) 在后面板电源插座上插上电源线，打开电源开关，前面板的 Power 灯(绿色，电源指示灯)，说明设备正常工作。

(2) 用标准 RJ-45 以太网线将 eth0 口与内部局域网连接。

1.5 登录设备

设备默认使用 eth0 作为管理口，eth0 出厂 IP 地址为 192.168.15.2/24，设备采用安全的 HTTPS 登录，默认端口 443。初始登录 URL 为：https://192.168.15.2，首次访问该地址需要导入授权（授权相关，详见配置指导书）。

授权产品类型：硬件版、软件版、云模式-认证中心授权。

1. 硬件版

导入硬件版授权证书。

图1-1 激活授权

2. 软件版

在左侧【单机模式授权】，导入软件版授权证书。

图1-2 激活授权

授权导入成功，重新访问 https://192.168.15.2 页面。默认的管理员账号是 admin，密码是 admin。正确输入用户名、密码及验证码后，点击<登录>按钮即可进入管理界面，如下图所示。

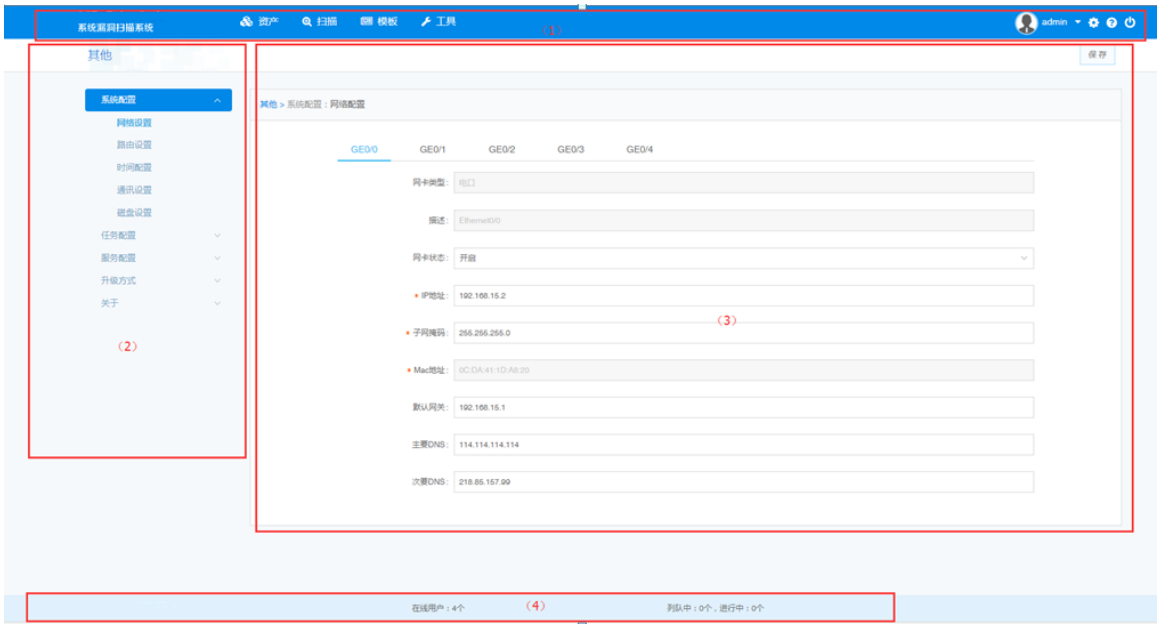
图1-3 管理员登录界面

提示

- 验证码为字母和数字，区分大小字母。
- 如果系统账号密码输错 5 次，缺省情况下，系统账号将被锁定 3 分钟。

1.6 Web网管页面布局

图1-4 Web 网管页面布局

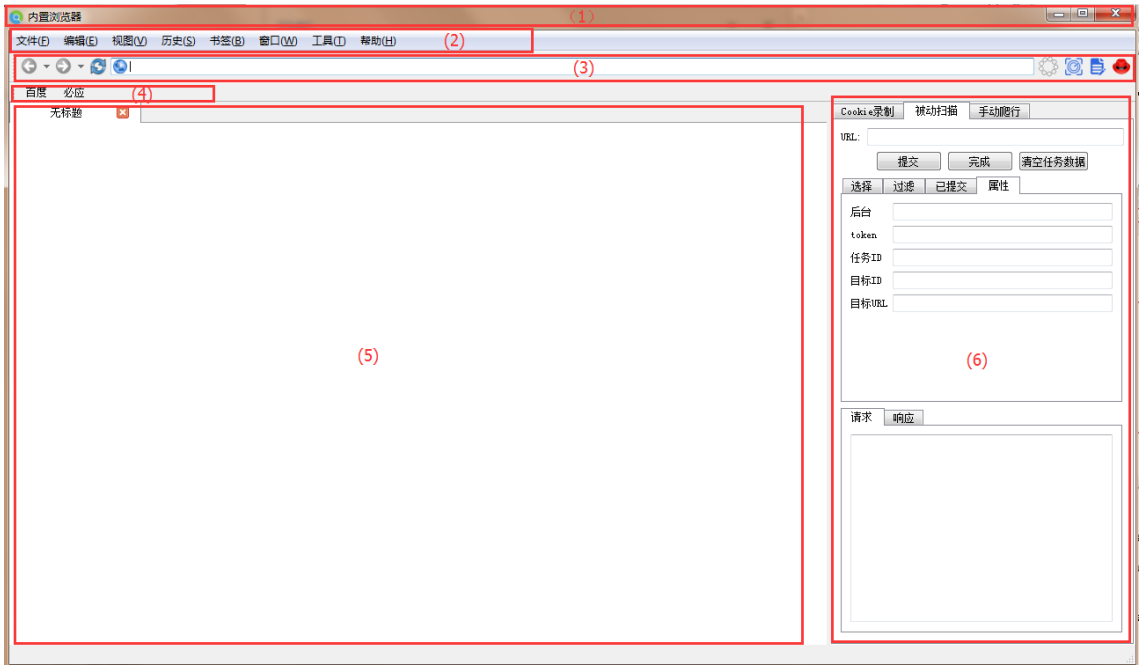


(1) 菜单栏	(2) 导航栏	(3) 配置区	(4) 状态栏

- 菜单栏：以不同的角度提供了各类管理功能的配置入口，方便用户根据实际需要进行切换。
- 导航栏:以导航树的形式组织设备的 Web 网管功能菜单,用户在导航栏中可以方便的选择功。能菜单，选中功能菜单的页面显示在配置区中。
- 配置区：用户进行配置和查看的区域。
- 状态栏：包括在线用户数和扫描任务调度数量统计。

1.7 系统专用浏览器页面布局

图1-5 系统专用浏览器页面布局



(1)标题栏	(2) 菜单栏	(3) 导航栏	(4) 书签栏	(5) 浏览器内容	(6) 工具集

- 标题栏：主要包括标题、最小化、最大化、关闭按钮。
- 菜单栏：主要包括文件、编辑、视图、历史、书签、窗口、工具、帮助。
- 导航栏：包括浏览器前进、后退、刷新、URL 地址、加载动态图标、工具集显示切换开关、菜单栏切换显示开关、渗透测试工具入口。
- 书签栏：可通过右键点击导航栏区域，选择需要的功能显示。
- 浏览器内容：浏览器内容显示区域。
- 工具集：工具集显示区域，可通过(5)和(6)之间的拖动线改变两者显示的比例。

2 资产管理

用户通过资产管理功能可以对目标网络中的所有信息资产进行资产风险管理。提供主机、数据库、Web 资产的新建、编辑、修改、删除、导入、导出、生成报表、资产统计及资产信息展示等功能，用户新增扫描任务时，可从资产列表中导入扫描目标。

图2-1 资产管理

2.1 新建资产

2.1.1 新建主机资产

功能描述：【新增主机资产】模块中包括【基本信息】、【认证设置】。

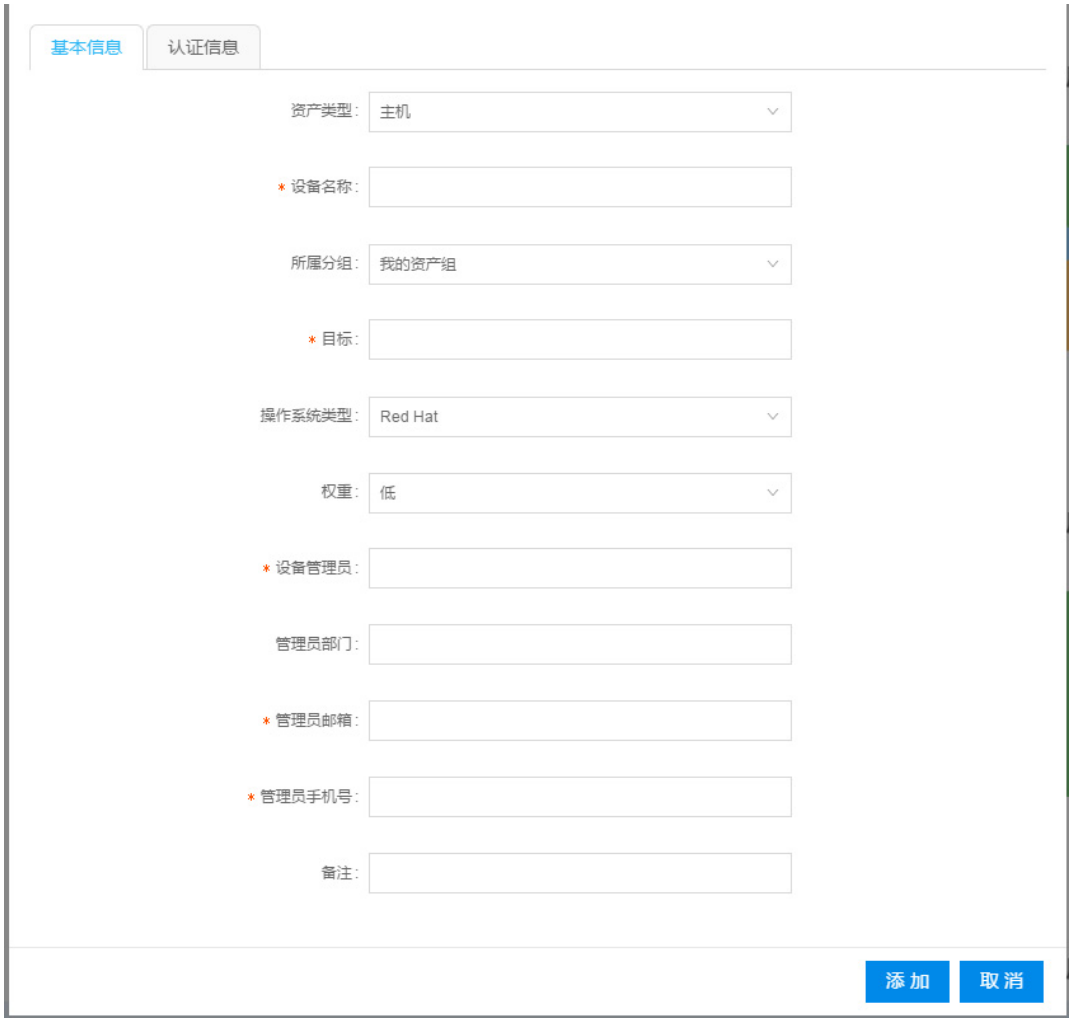
配置路径：【资产】>【资产管理器】>【新建资产】

1. 基本信息

功能描述：提供资产基本信息的配置。

配置路径：【资产】>【资产管理器】>【新建资产】>【基本信息】

图2-2 主机资产基本信息



参数说明：

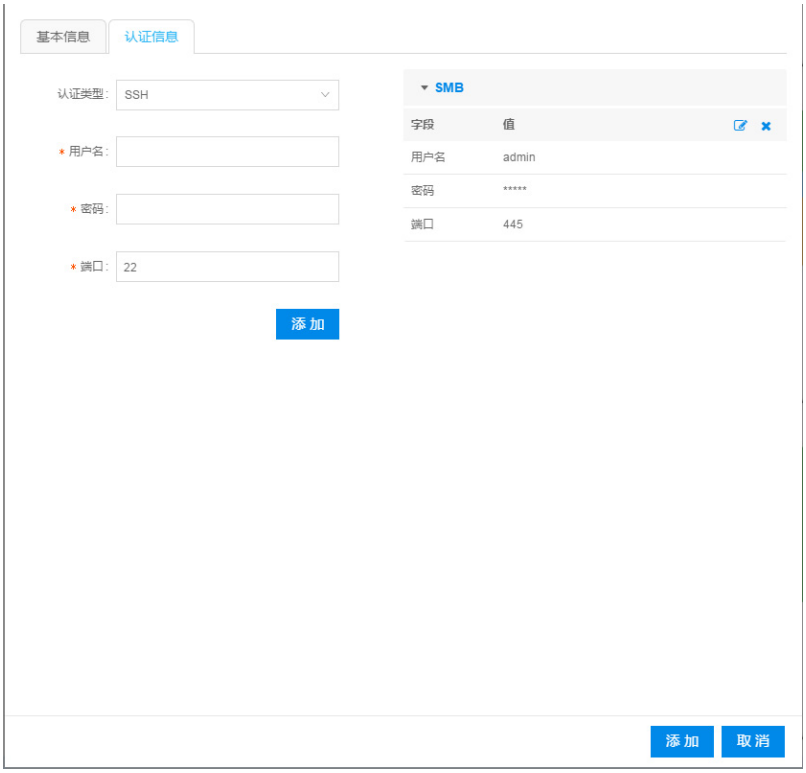
- <资产类型>：选择主机。
- <设备名称>：资产的名称。
- <所属分组>：该资产所属的资产组。
- <目标>：该资产的 IP 地址。
- <操作系统类型>：该资产的操作系统类型。
- <权重>：主机和网络风险等级计算时所采用的变量，权重越高资产越重要，计算出来的风险等级越高。
- <设备管理员>：该资产的设备管理员。
- <管理员部门>：该资产管理员的部门。
- <管理员邮箱>：该资产管理员的邮箱。
- <管理员手机号>：该资产管理员的手机号。
- <备注>：备注信息。

2. 认证信息

功能描述：提供资产认证信息的配置。

配置路径：【资产】>【资产管理器】>【新建资产】>【认证信息】

图2-3 主机资产认证信息



参数说明：

- <认证类型>：选择资产的认证协议，支持 SMB、SSH、TELNET 三种协议的认证。
- <用户名>：该认证协议的用户名。
- <密码>：该认证协议的密码。
- <端口>：该认证协议的端口。
- <编辑认证>：点击子任务“操作”栏目下的 可以对认证进行编辑。
- <删除认证>：点击 ，可删除认证。

2.1.2 新建Web资产

功能描述：【新增 Web 资产】模块中包括【基本信息】。

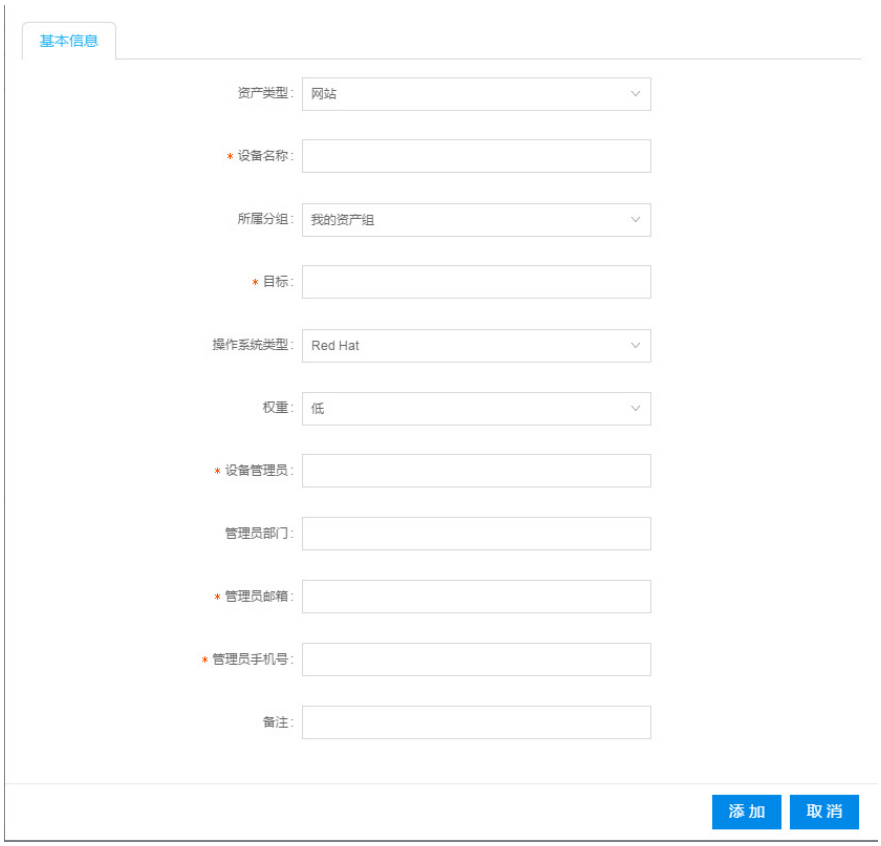
配置路径：【资产】>【资产管理器】>【新建资产】

1. 基本信息

功能描述：提供资产基本信息的配置。

配置路径：【资产】>【资产管理器】>【新建资产】>【基本信息】

图2-4 Web 资产基本信息 Web 资产基本信息



参数说明：

- <资产类型>：选择网站。
- <设备名称>：资产的名称。
- <所属分组>：该资产所属的资产组。
- <目标>：该资产的网站地址。
- <操作系统类型>：该资产的操作系统类型。
- <权重>：主机和网络风险等级计算时所采用的变量，权重越高资产越重要，计算出
- <设备管理员>：该资产的设备管理员。
- <管理员部门>：该资产管理员的部门。
- <管理员邮箱>：该资产管理员的邮箱。
- <管理员手机号>：该资产管理员的手机号。
- <备注>：备注信息。

2.1.3 新建数据库资产

功能描述：【新增数据库资产】模块中包括【基本信息】、【认证设置】。

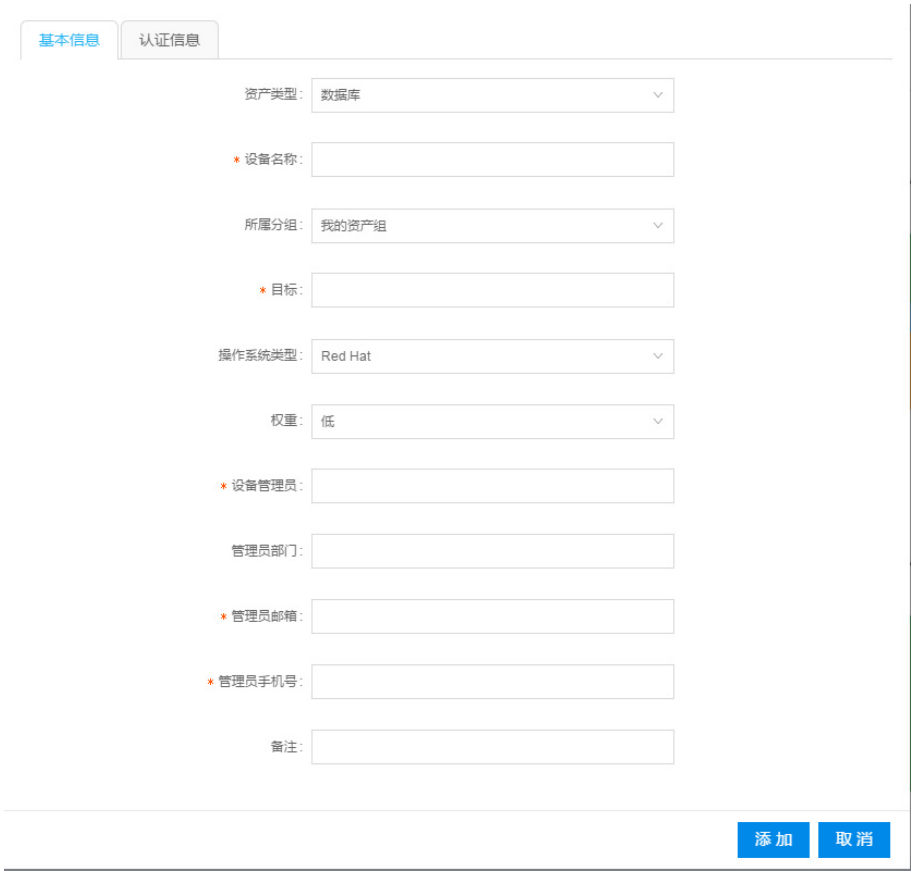
配置路径：【资产】>【资产管理器】>【新建资产】

1. 基本信息

功能描述：提供资产基本信息的配置。

配置路径：【资产】>【资产管理器】>【新建资产】>【基本信息】

图2-5 数据库资产基本信息



参数说明：

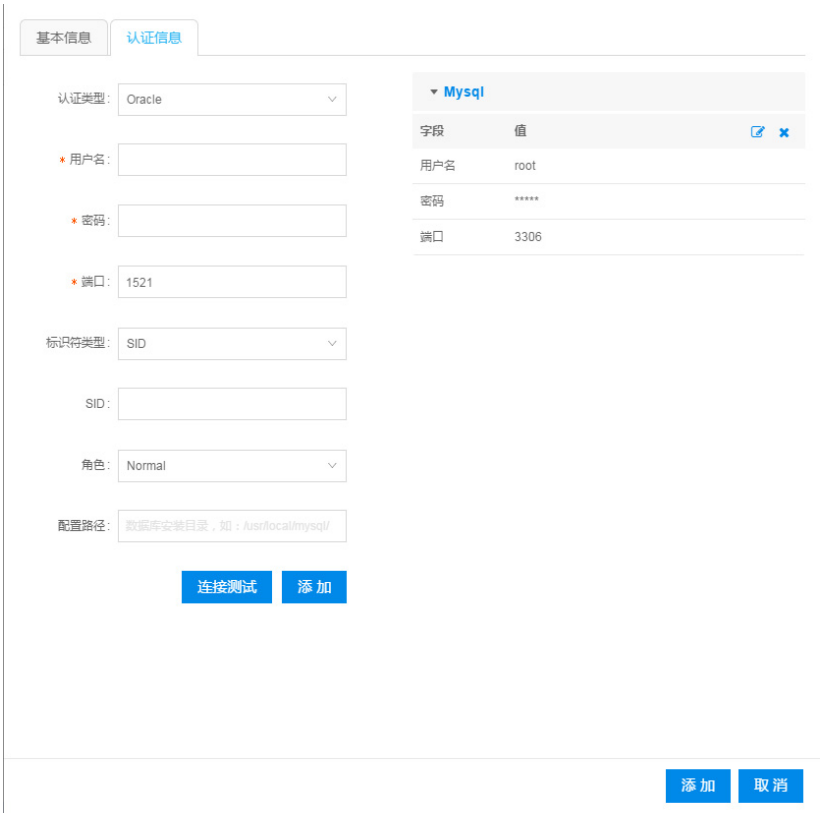
- <资产类型>：选择数据库。
- <设备名称>：资产的名称。
- <所属分组>：该资产所属的资产组。
- <目标>：该资产的 IP 地址。
- <操作系统类型>：该资产的操作系统类型；
- <权重>：主机和网络风险等级计算时所采用的变量，权重越高资产越重要，计算出
- <设备管理员>：该资产的设备管理员。
- <管理员部门>：该资产管理员的部门。
- <管理员邮箱>：该资产管理员的邮箱。
- <管理员手机号>：该资产管理员的手机号。
- <备注>：备注信息。

2. 认证信息

功能描述：提供资产认证信息的配置。

配置路径：【资产】>【资产管理器】>【新建资产】>【认证信息】

图2-6 数据库资产认证信息



参数说明：

- <认证类型>：选择资产的认证协议，支持 SMB、SSH、Telnet、Mysql、Oracle、SqlServer、DB2、Informix、Sybase、DM 协议的认证。
- <用户名>：该认证协议的用户名。
- <密码>：该认证协议的密码。
- <端口>：该认证协议的端口。
- <标识符类型>：该 Oracle 标识符类型，根据需求选择 SID 或数据库名称。
- <SID>：Oracle 数据库的 SID。
- <数据库名称>：该认证协议数据库名称。
- <服务名称>：该认证协议数据库服务名称。
- <配置路径>：该认证协议数据库安装目录。
- <连接测试>：验证数据库是否可登录成功。
- <编辑认证>点击子任务“操作”栏目下的 可以对认证进行编辑。
- <删除认证>：点击 ，可删除认证。

2.1.4 新建资产组

功能描述：提供资产基本信息的配置。

配置路径：【资产】>【资产管理器】>【新建资产组】

图2-7 资产组-新建

参数说明：

- <分组名称>：资产分组名称。
- <所在分组>：该资产分组的父组。

2.2 资产管理

功能描述：用户还可以对资产及资产组进行修改、删除和新建任务及生成报表等操作，对资产树进行导入和导出等操作。

配置路径：【资产】>【资产管理器】如下图所示。

图2-8 资产管理器

2.2.1 编辑资产

点击资产上的 可以对资产进行编辑，资产类型不允许编辑。

2.2.2 编辑资产组

点击资产组上的 可以对资产组进行编辑。

2.2.3 删除资产

点击资产上的 即可删除对应的资产，删除任务有二次确认提示，请确认是否进行删除。

2.2.4 删除资产组

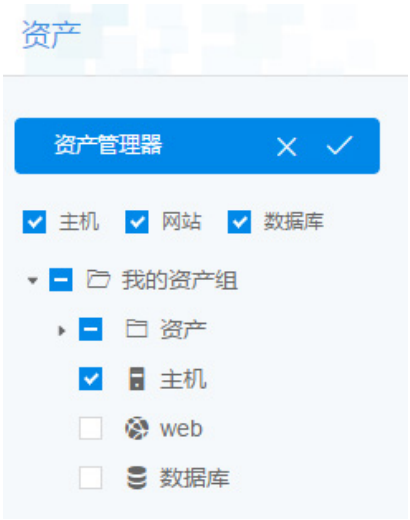
点击资产组上的 即可删除对应的资产组且清空资产分组下资产数据，删除任务有二次确认提示，请确认是否进行删除。

2.2.5 新建任务

配置路径：【资产】>【资产管理器】>【新建任务】

选择勾选需要的资产，点击 。

图2-9 新建任务



跳转至新建任务模块，如下图。详见 3.1 章节新增任务。

图2-10 任务编辑

提示

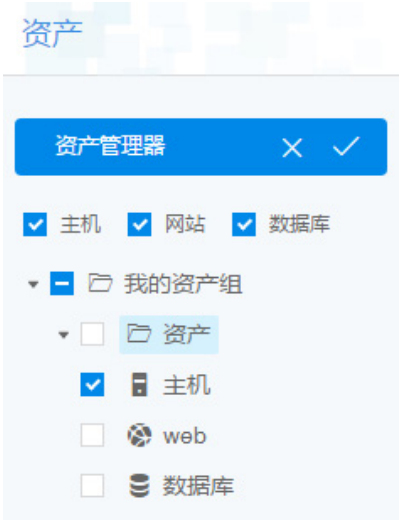
- 只能选择一种类型资产进行新建任务；
- 跳转到新建任务模块，该资产的目标及认证设置自动填入对应的扫描目标和认证设置。

2.2.6 生成报表

配置路径：【资产】>【资产管理器】>【生成报表】

选择勾选需要生成报表的资产，点击  。

图2-11 生成报表



弹出报表下载窗口，如下图。

图2-12 报表下载

2.2.7 资产模板下载

配置路径：【资产】>【资产管理器】>【资产模板下载】

点击【资产模板下载】，下载一个资产模板 xls 的文件

2.2.8 资产导出

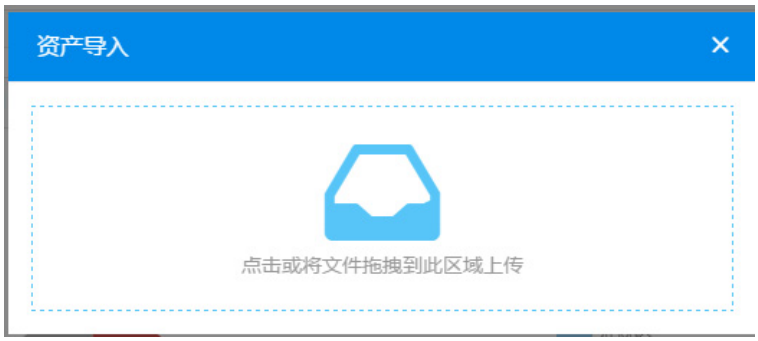
配置路径：【资产】>【资产管理器】>【资产导出】

点击【资产导出】，把全部资产信息导出成一个 xls 的文件。

2.2.9 资产导入

配置路径：【资产】>【资产管理器】>【资产导入】

图2-13 资产导入



导入的前提要将相应的资产模板导出，选择要导入的策略模板文件或拖动要导入的文件至导入区域；如果导入的模版损坏或格式不正确则会给出相应的提示。

提示

导入资产成功后，同时覆盖原有资产组、资产，清空所有资产配置。

2.3 资产组展示

功能描述：从资产管理视图快速定位所有目标资产的风险等级、漏洞分布、严重程度、影响区域，直观展示安全风险及风险统计信息，而不是以任务为导向来展示漏洞信息。

2.3.1 资产组展示

配置路径：【资产】>【资产管理器】

选中需要统计展示的资产组，查看右侧资产信息汇总展示，如下图。

图2-14 资产组展示

1. 综述信息

配置路径：【资产】>【资产管理器】>【综述信息】

点击【综述信息】，显示主机，网站，数据库目标资产漏洞风险的统计图和目标资产的风险分布图（即风险等级的统计图）。

2. 资产信息

配置路径：【资产】>【资产管理器】>【资产信息】

点击【资产信息】，显示主机、网站、数据库目标资产漏洞信息列表，属性包含目标、设备名称、最后扫描时间、漏洞风险个数(紧急、高风险、中风险、低风险、信息、合计)、风险等级。

点击等级的 ，进行漏洞级别的过滤功能，如果只勾选紧急风险，就显示存在紧急风险漏洞的目标资产。点击风险等级的 ，对风险等级进行排序。

3. 主机漏洞

配置路径：【资产】>【资产管理器】>【主机漏洞】

点击【主机漏洞】，显示主机目标资产风险等级列表，属性包含等级、编号、名称、影响主机比例、出现次数。

点击漏洞等级的  ，进行漏洞级别的过滤功能，如果只勾选紧急，就显示存在紧急漏洞的目标资产。点击风险等级的  ，对漏洞等级进行排序。

点击“+”展开后的截图，显示受影响的主机目标资产；点击名称，跳转至主机漏洞详情页面。

4. 网站漏洞

配置路径：【资产】>【资产管理器】>【网站漏洞】

点击【网站漏洞】，显示网站目标资产风险等级列表，属性包含等级、编号、名称、影响主机比例、出现次数。

点击漏洞等级的  ，进行漏洞级别的过滤功能，如果只勾选紧急，就显示存在紧急漏洞的目标资产。点击风险等级的  ，对漏洞等级进行排序。

点击“+”展开后的截图，显示受影响的网站目标资产；点击名称，跳转至网站漏洞详情页面。

5. 数据库漏洞

配置路径：【资产】>【资产管理器】>【数据库漏洞】

点击【数据库漏洞】，显示数据库目标资产风险等级列表，属性包含等级、编号、名称、影响主机比例、出现次数。

点击漏洞等级的  ，进行漏洞级别的过滤功能，如果只勾选紧急，就显示存在紧急漏洞的目标资产。点击风险等级的  ，对漏洞等级进行排序。

点击“+”展开后的截图，显示受影响的数据库目标资产；点击名称，跳转至主机漏洞详情页面。

2.3.2 资产展示

配置路径：【资产】>【资产管理器】

选中需要统计展示的资产，查看右侧资产信息汇总展示，如下图。

图2-15 资产展示

1. 基本信息

配置路径：【资产】>【资产管理器】>【基本信息】

点击【基本信息】，显示目标资产的基本信息。

2. 漏洞列表

配置路径：【资产】>【资产管理器】>【漏洞列表】

点击【漏洞列表】，显示目标资产风险等级列表，属性包含等级、标识、名称、次数。

点击漏洞等级的  ，进行漏洞级别的过滤功能，如果只勾选紧急，就显示存在紧急漏洞的目标资产；点击风险等级的  ，对漏洞等级进行排序；点击名称，跳转至漏洞详情页面。

3 扫描

“扫描”包新增任务、任务管理、扫描参数、对比分析、扫描基本配置、定时扫描、普通扫描、对象管理、报告下载等功能。

3.1 新增任务

【新增任务】模块中包括【基本配置】、【主机扫描参数】、【Web 扫描参数】、【数据库扫描参数】、【主机通知参数】。

3.1.1 基本配置

功能描述：创建扫描任务及其相关的基本配置，包含基本参数、主机扫描、Web 扫描的配置。

配置路径：【扫描】>【新增任务】>【基本配置】

1. 基本参数

功能描述：提供扫描任务基本参数的配置。

配置路径：【扫描】>【新增任务】>【基本配置】>【基本参数】

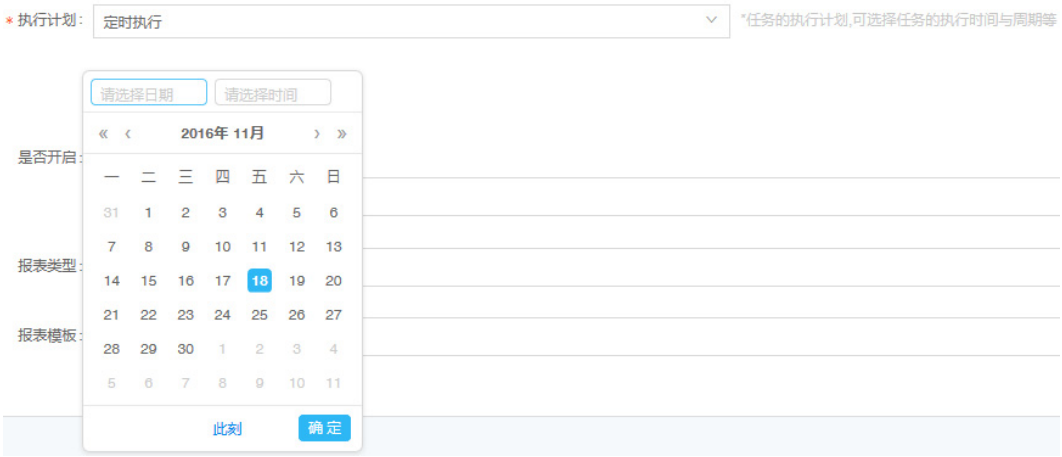
图3-1 任务编辑界面

参数说明：

- <任务名称>：扫描任务名称不能为空，支持中文、英文、数字、符号或四种者组合。
- <任务分组>：支持任务分组的新建，可将不同类型的扫描任务分配到相应的任务分组。
- <扫描类型>：扫描类型支持主机扫描、Web 扫描、数据库扫描，默认选中主机扫描，左侧列表展示主机扫描相关参数，选中 Web 扫描时，则自动出现 web 扫描相关的参数，选中数据库扫描时，则自动出现数据库扫描相关的参数。

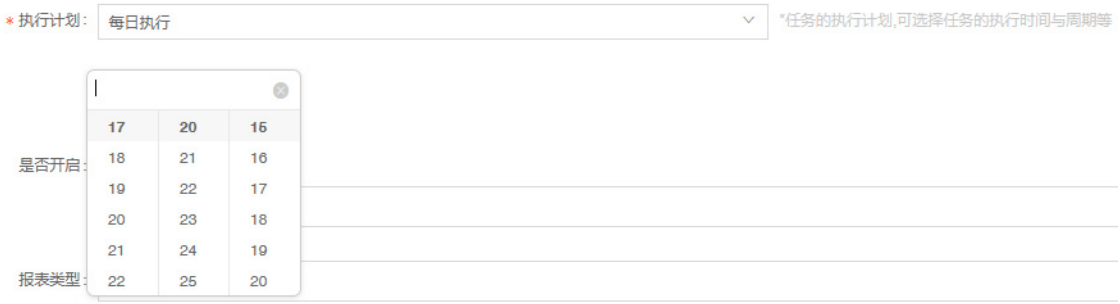
- <优先级>：系统内置高中低三个不同优先级，缺省为“中”优先级，扫描优先级顺序依次为高>中>低，可通过鼠标点击单选按钮调整优先级。
- <执行计划>：任务的执行计划系指可选择任务的执行时间与周期等，包括立即执行、暂不执行、定时执行、每日执行、每周执行、每月执行等六个选项。
- <发送结果到邮箱>：开启【发送结果】功能，则在已设置 SMTP 服务的前提下，系统能将扫描结果按照设定的报表类型和报表模板发送到指定的邮箱。
- <上传结果到 FTP>：开启【传结果到 FTP】功能，则在已设置 FTP 服务器的前提下，系统能将扫描结果按照设定的报表类型和报表模板上传到指定的 FTP 目录。
- <报表类型>：选择导出的报表类型，对应的报表类型有 html 报表，word 报表以及 pdf 报表三种格式。
- <报表模板>：主机和数据库扫描任务对应的默认模板有 3 种，分别是技术工程师、安全工程师、行政主管；web 扫描任务对应的默认模板有 7 种，分别是技术工程师、安全工程师、行政主管、OWASP TOP10 2013 版、等级保护报表 2 级、等级保护报表 3 级、等级保护报表 4 级；不同的报表模板展示内容有所不同，此功能可在【模板】>【报表模板】>设定，具体设置见 4.3 章节报表模板说明。
- <保存>：点击【保存】，完成扫描任务配置。
- <返回>：点击【返回】，取消新建扫描任务。
- <立即执行>指创建完扫描任务后，即刻开始执行扫描任务；
- <暂不执行>提创建完扫描任务后，不执行扫描任务，可通过【任务管理】按需要执行扫描任务，详细见“3.2 章节”任务管理。
- <定时执行>指根据管理员需要，指定具体时间执行扫描任务，点击右侧的“ ”图标，可以选择具体的时间，如下图所示。

图3-2 任务编辑-定时执行



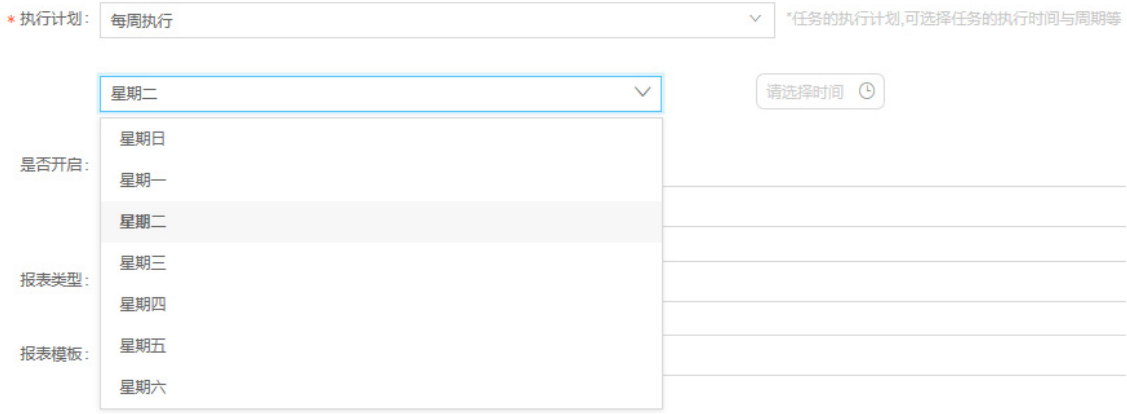
- <每日执行>指根据管理员需要，每天到指定时间点，系统自动开始执行相应的扫描任务。点击右侧的“ ”图标，可以选择具体的时间，如下图所示。

图3-3 任务编辑-每日执行



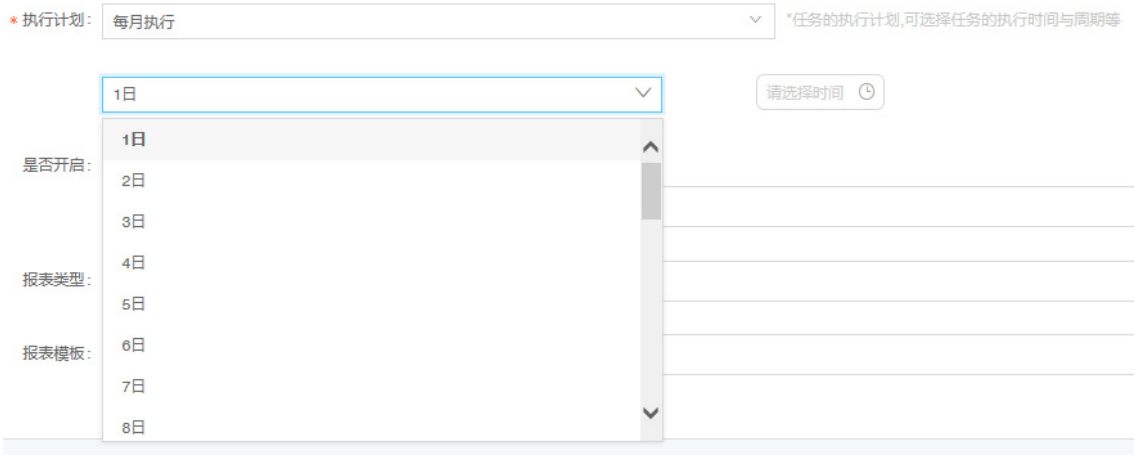
- <每周执行>指以星期为周期，指根据管理员需要每个星期到指定时间点，系统自动开始周期性执行相应的扫描任务。点击右侧的“ ”图标，可以选择具体的时间，如下图所示。

图3-4 任务编辑-每周执行



- <每月执行>指以月为周期，指根据管理员设定的日期，系统自动开始周期性执行相应的扫描任务。点击右侧的 标，可以选择具体的时间，如下图所示。

图3-5 任务编辑-每月执行



提示

- “定时执行”需要选择年-月-日时-分-秒，精确到秒的具体时间点，如 2016-09-29 19:00:00。
- “每日执行”无须选择日期，只要选择到时-分-秒即可，如 19:00:00 表示每天 19：00：00 系统自动执行该扫描任务。
- “每周执行”需选择星期几及具体的时间点，如星期二 19：00：00 表示每星期二 19：00：00 自动执行扫描任务。
- “每月执行”需要选择每月几号及具体时间点，如 19 号 19：00：00 表示每月 19 号 19：00：00 自动执行扫描任务。

2. 主机扫描

功能描述：提供主机扫描目标相关配置。

配置路径：【扫描】>【新增任务】>【基本配置】>【主机扫描】

图3-6 任务编辑-新增主机扫描目标

参数说明：

- <扫描目标>：扫描目标支持手工填写扫描目标 IP、IP 范围、域名；支持按下载的模板格式要求填写扫描目标，并通过<从模板导入>导入文件；也可以通过<从资产导入>导入扫描目标。

提示

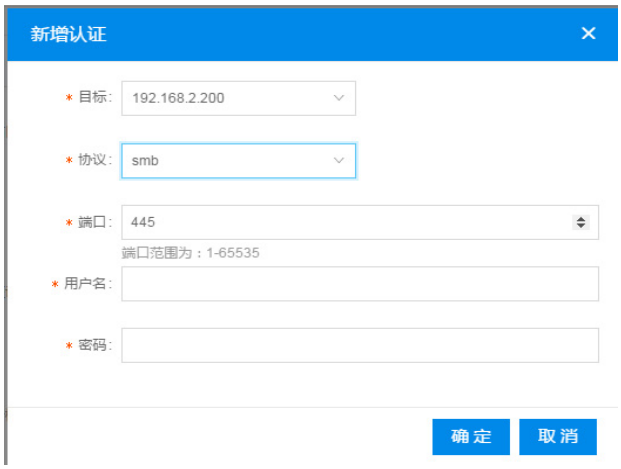
- 扫描目标支持单个 IP、IP 范围等，同时扫描多个目标时，通过逗号（,）隔开。
- 192.168.1.1 到 192.168.1254；192.168.*.*表示 192.168 开头的所有 IP，*.baidu.com 表示域名为 baidu.com 的所有目标。
- 扫描目标填写域名时，需要配置正确的 DNS，否则会影响扫描结果。
- 符号若无特殊说明，此用户手册以及系统一律是使用半角字符。

- <认证设置>：在填写完<扫描目标>后，会自动出现<认证设置>，认证设置支持 SMB、SSH、TELNET 三种协议的认证，通过认证设置可以提高扫描精确度与深度。支持<导入认证>与<手动添加>两种设置方式，<认证下载>提供认证模板的下载。
- <策略模板>：系统缺省扫描策略为“完全扫描”，可通过<选择模板>可以选择系统自带模板，以便选择有针对性的扫描策略。策略模板具体配置详见“4.1 策略模板”章节内容。
- <参数模板>：系统自带参数模板包括“默认参数”、“快速扫描”、“全面扫描”。详细配置见“4.2 参数模板”章节内容。
- <导入认证>：导入的前提要将相应的认证模板，选择要导入的认证模板或拖动要导入的文件至导入区域；如果导入的模版损坏或格式不正确则会给出相应的提示。

图3-7 任务编辑-认证导入

- <手动添加>通过下拉菜单选择目标地址、端口、用户名、密码等信息，输入完成后点击<确定>，完成添加认证。

图3-8 任务编辑-手动添加认证界面



- <认证下载>：提供认证模板下载，模板格式如下

图3-9 任务编辑-认证表

H3C SecPath 系统漏洞扫描系统_认证表

序号	IP地址	协议	端口	用户名	密码	数据库名称	数据库sid	配置路径	数据库 角色/服务名称
1									
2									
3									
4									
5									
6									
7									
8									

说明

1、IP地址格式范例：192.168.168.3-25,192.168.168.*,baidu.com!

2、同一个IP/IP段存在多个协议认证，请分成多行进行记录!

3、目前支持登录的协议有：SMB、SSH、Telnet、Mysql、Oracle、SqlServer、DB2、Informix、Sybase、DM!

4、默认协议端口 SMB:445, SSH:22, Telnet:23, Mysql:3306, Oracle:1521, SqlServer:1433, DB2:50000, Informix:1533, Sybase:5000, DM:5236 。

5、Oracle协议中的数据库名称和数据库sid填写其中一个即可，若两个都填写则只保留sid。

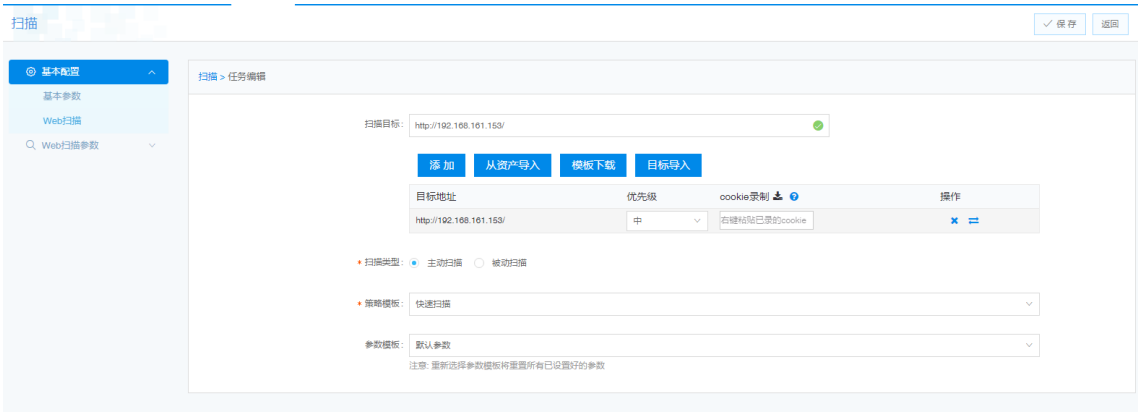
提示

- 当前仅支持 SMB、SSH、TELNET 三种协议认证。
- 输入不在扫描范围内的 IP 地址时候，系统会自动排除错误 IP。

3. Web扫描

配置路径：【扫描】>【新增任务】>【基本配置】>【Web 扫描】

图3-10 任务编辑-新增 Web 扫描目标



参数说明：

- <扫描目标>：支持手动添加及从资产导入，目标模板导入三种模式；在输入框中输入需要扫描的网站地址，
- <添加>：可将目标网站添加到扫描目标列表。
- <从资产导入>：将网站资产导入到扫描目标列表。
- <模板下载>：下载 Web 扫描目标模板，在模板中输入目标 URL。模板格式如下。

图3-11 Web 扫描目标模板 Web 扫描目标模板

Web扫描目标输入格式说明
注：（每个扫描目标路径独自取一行一列，扫描目标以"http://"或"https://"作为前缀）

- <目标导入>：上传模板文件导入 Web 扫描目标。
- <优先级>：内置高中低三个不同优先级，缺省为“中”优先级，扫描优先级顺序依次为高>中>低，可通过鼠标点击单选按钮调整优先级。

- <cookie 录制>：点击 下载内置浏览器，打开工具浏览要扫描的网站，获取用户登录操作后的相关信息，如 COOKIE 或 SESSION，保存 cookie 后右键黏贴到 cookie 输入框，保存扫描任务后，扫描器可对业务系统深度扫描，帮助用户发现更多的网站漏洞。

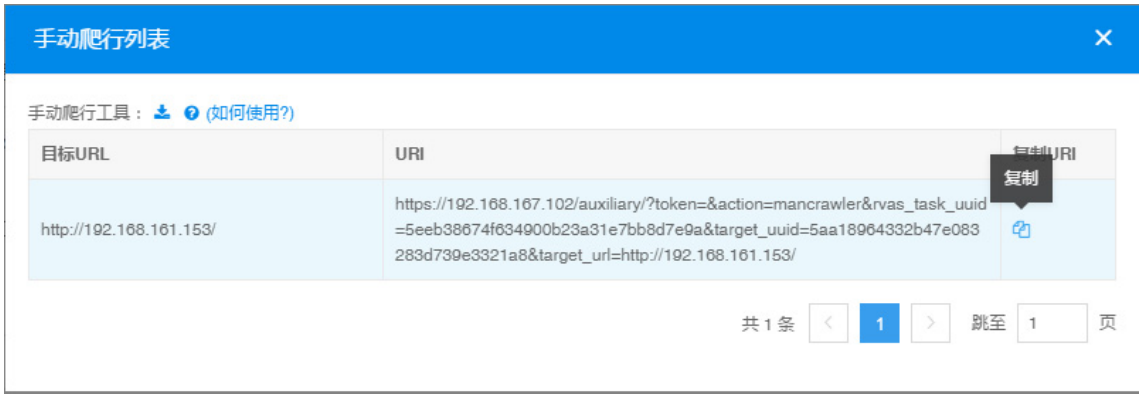
提示

击【cookie 录制】旁的 按钮，根据页面上的提示步骤进行设置。

- <删除>：点击目标列表操作列的 ，可删除扫描的目标。
- <检测网站>：点击目标列表操作列的 ，可检测添加的扫描目标是否可正常访问。
- <扫描类型>：支持主动扫描和被动扫描两种扫描方式。可以通过下载内置浏览器，通过浏览器中被动扫描和手动爬行功能实现不同扫描方式。
- <策略模板>：系统缺省扫描策略为“快速扫描”，可通过<选择模板>可以选择系统自带模板，以便选择有针对性的扫描策略。策略模板具体配置详见“4.1 策略模板”章节内容。
- <参数模板>：系统自带参数模板包括“默认参数”、“webgoat 7.0”、“webgoat 5.4”。详细配置见“4.2 参数模板”章节内容。
- <手动爬行>：新建子任务，执行计划选择<暂不执行>，扫描类型选择<主动扫描>，点击子任务<操作>栏目下的 。

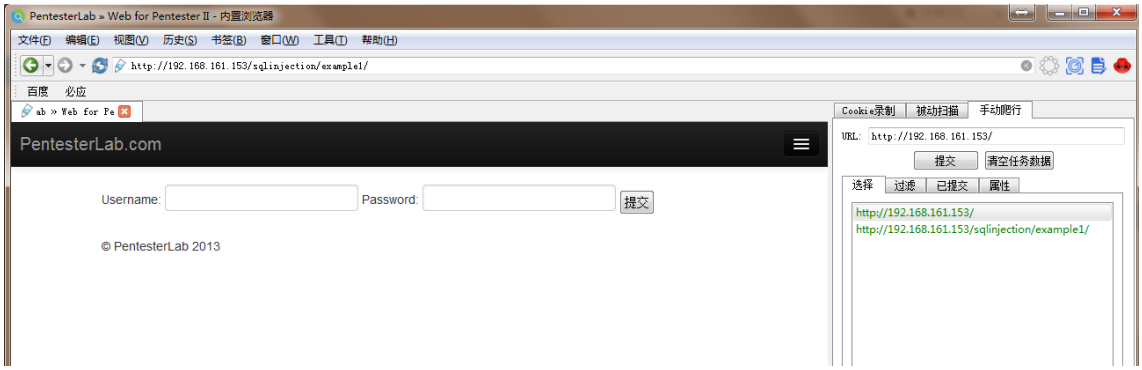
图3-12 手动爬行

图3-13 手动爬行列表



将复制好的 URI 内容粘贴到内置浏览器的地址栏，并回车；通过内置浏览器用户进行手动点击想要检测页面的 URL，点击【提交】按钮，扫描器自动保存所有手动爬行的 URL。详情请参见 7.4 章节手动爬行。

图3-14 内置浏览器-手动爬行



- <被动扫描>：新建子任务，执行计划选择“暂不执行”，扫描类型选择“被动扫描”，点击子任务“操作”栏目下的 。

图3-15 被动爬行

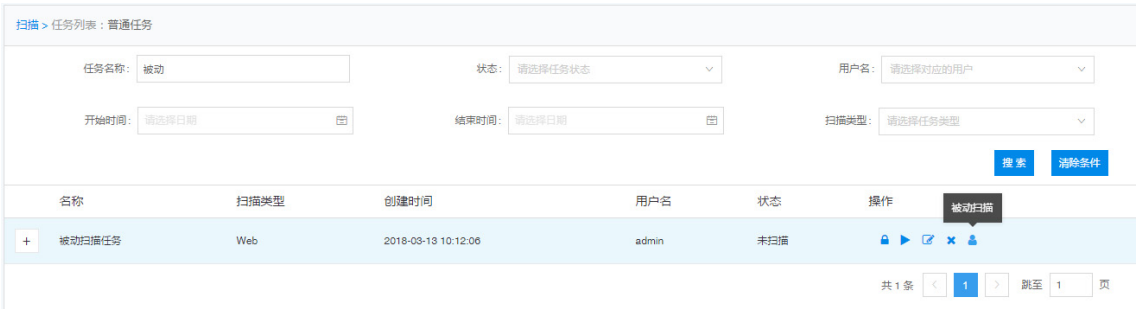
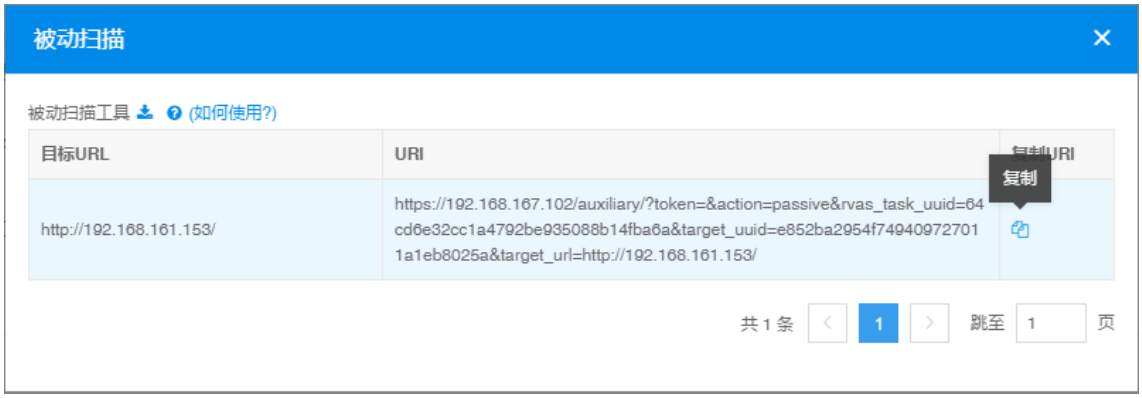
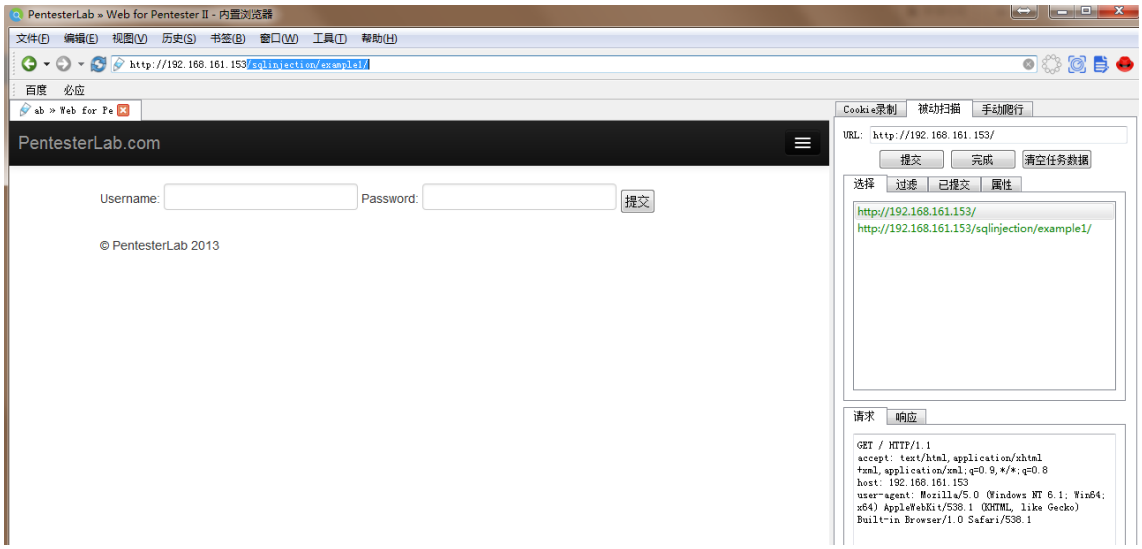


图3-16 被动爬行



将复制好的 URI 内容粘贴到内置浏览器的地址栏，并回车；通过内置浏览器，用户手动点击要检测页面的 URL，既可以多次点击【提交】按钮进行提交 URL，也可以最后一次性提交 URL，点击【完成】按钮，扫描器将对所有提交的 URL 进行漏洞检测。详情请参见 7.3 章节被动爬行。

图3-17 内置浏览器-被动爬行



4. 数据库扫描

功能描述：提供数据库扫描目标相关配置。

配置路径：【扫描】>【新增任务】>【基本配置】>【扫描】

图3-18 任务编辑-新增数据库扫描目标

参数说明：

- <扫描目标>：扫描目标支持手工填写扫描目标 IP、IP 范围、域名；支持按下载的模板格式要求填写扫描目标，并通过<从模板导入>导入文件；也可以通过<从资产导入>导入扫描目录。

提示

- 扫描目标支持单个 IP、IP 范围等，同时扫描多个目标时，通过逗号（,）隔开。
- 192.168.1.1 到 192.168.1254；192.168.*.*表示 192.168 开头的所有 IP，*.baidu.com 表示域名为 baidu.com 的所有目标。
- 扫描目标填写域名时，需要配置正确的 DNS，否则会影响扫描结果。
- 符号若无特殊说明，此用户手册以及系统一律是使用半角字符。

- <认证设置>：在填写完<扫描目标>后，会自动出现认证设置，认证设置支持 SMB、SSH、Telnet、Mysql、Oracle、SqlServer、DB2、Informix、Sybase、DM 协议的认证，通过认证设置可以提高扫描精确度与深度。支持【导入认证】与【手动添加】两种设置方式，【认证下载】提供认证模板的下载。
- <策略模板>：系统缺省扫描策略为“数据库完全检测”，可通过<选择模板>可以选择系统自带模板，以便选择有针对性的扫描策略。策略模板具体配置详见“4.1 策略模板”章节内容。
- <参数模板>：系统自带参数模板包括“默认参数”、“快速扫描”、“全面扫描”。详细配置见“4.2 参数模板”章节内容。
- <导入认证>：导入的前提要将相应的认证模板，选择要导入的认证模板或拖动要导入的文件至导入区域；如果导入的模版损坏或格式不正确则会给出相应的提示。

图3-19 任务编辑-认证导入

- <手动添加>：通过下拉菜单选择目标地址、端口、用户名、密码等信息，输入完成后点击<确定>，完成添加认证。

图3-20 任务编辑-手动添加认证界面

- <认证下载>：提供认证模板下载，模板格式如下：

图3-21 任务编辑-认证表

系统漏洞扫描系统 认证表

序号	IP地址	协议	端口	用户名	密码	数据库名称	数据库sid	配置路径	数据库 角色/服务名称
1									
2									
3									
4									
5									
6									
7									
8									

说明

1、IP地址格式范例：192.168.168.3-25,192.168.168.*,baidu.com；

2、同一个IP/IP段存在多个协议认证，请分成多行进行记录；

3、目前支持登录的协议有：SMB、SSH、Telnet、Mysql、Oracle、SqlServer、DB2、Informix、Sybase、DM；

4、默认协议端口 SMB:445, SSH:22, Telnet:23, Mysql:3306, Oracle:1521, SqlServer:1433, DB2:50000, Informix:1533, Sybase:5000, DM:5236 。

5、Oracle协议中的数据库名称和数据库sid填写其中一个即可，若两个都填写则只保留sid。

提示

- 目标协议端口为默认端口，认证参数表格中的端口可以为空。
- 当前仅支持 SMB、SSH、Telnet、Mysql、Oracle、SqlServer、DB2、Informix、Sybase、DM 协议认证。
- 输入不在扫描范围内的 IP 地址时候，系统会自动排除错误 IP。

3.1.2 主机扫描参数

功能描述：提供常规参数、端口参数、破解参数等扫描参数配置。

配置路径：【扫描】>【新增任务】>【主机扫描参数】

1. 常规参数

功能描述：提供扫描线程数、允许同时扫描主机数、扫描方式、漏洞扫描参数等扫描参数的配置。

配置路径：【扫描】>【新增任务】>【主机扫描参数】>【常规参数】，配置界面如下图所示。

图3-22 主机扫描参数-常规参数配置

参数说明：

- <扫描进程数>：系统进行漏洞扫描时，扫描引擎将启动的最大扫描并发进程数量。扫描进程数与所需的系统资源数成正比，扫描进程数越大，扫描效率越高，其所需的系统资源也就越多。但并非扫描进程数越大越好，到达一定数目后增加进程数对扫描速度的提高作用有限，反而浪费系统资源。此参数的允许范围和默认优化值因产品型号不同而不同。
- <允许同时扫描主机数>：系统最大主机扫描并发数量。允许并发扫描主机数越多，系统的扫描效率越高，但主机数到达一定数目后，将增加系统的负荷，系统效率提高有限。此参数的允许范围和默认优化值因产品型号不同而不同。
- <脚本检测超时时间>：是指单个漏洞脚本的执行时间若超过“脚本检测超时时间”则会停止对该漏洞项的扫描，以加快扫描速度。该参数默认优化值为“60 秒”。
- <在线判断超时时间>：是指系统判断远程主机是否在线的时间阀值，系统在“在线判断超时日间”值内，未收到远程主机的响应，则判断远程主机不在线。
- <扫描方式>中的<强制扫描>指扫描引擎将不判断目标主机是否在线而直接对其进行漏洞扫描。若在<强制扫描>参数选项中选“否”，则系统在扫描时将先判断目标主机是否在线，若不在线则不对该主机进行扫描。此参数默认优化值为“否”。
- <报告级别>包含“精确”、“常规”、“全面”三个选项，其中“精确”，报告中仅包含根据漏洞原理识别风险的漏洞；“常规”，报告中排除根据据版本号识别风险外的所有漏洞；“全面”，报告中包含所有可能存在风险的漏洞。
- <调试模式>应用场景，用于原厂商工程师非现场情况下收集客户环境下脚本的调试信息，协助客户完成漏洞测试和确认。此参数默认优化值为“关闭”。
- <在线检测方法>指检测远程主机是否线的方法，包括 ICMP 和 ICMP+CONNECT 两种检测方法。ICMP 通过发送 ICMP 包给远程主机，ICMP+CONNECT 除了通过发送 ICMP 包外，还可通过 TCP 连接状态来判断远程主机是否在线，TCP 端口号通过逗号（,）隔开。

- <安全扫描>指系统在扫描远程主机漏洞的时候，不会对远程主机造成伤害的扫描方式。此参数默认优化值为“是”。

2. 端口参数

功能描述：包含 TCP 端口和 UDP 端口参数的配置。

配置路径：【扫描】>【新增任务】>【主机扫描参数】>【端口参数】，如下图所示。

图3-23 主机扫描参数-端口参数配置

TCP 参数说明：

- <扫描超时时间>：单个脚本的扫描超时时间，若等待超过设置的时间则系统会停止对该漏洞项的扫描，以加快扫描速度，超时时间可配置范围为 100 到 5000 毫秒，系统缺省值为 300 毫秒。
- <扫描范围设置>：支持典型端口、特殊端口、全部端口、自定义端口的设置，选中<典型端>只扫描一些常用的端口（可在【模板】>【数据字典】>【所有字典】>【端口字典】中查看）；选择<特殊端口>时扫描的端口范围是 1-1024；选择<全部端口>则扫描的端口范围为 1－65535；选中<不扫描>则不对 TCP 端口进行扫描；选中<自定义端口>后，用户可根据需要定义要扫描的 TCP 端口。
- <扫描方式设置>：扫描 TCP 端口时采用的扫描方式，包括 tcpconnect 和 tcpsync 两种扫描方式，其中 tcpconnect 通过 TCP 连接状态来判断远程主机是否有开放相应的 TCP 端口；tpcsync 通过是 TCP/IP 建立连接时使用的三次握手的状态来判断远程主机是否有开放相应的端口。

UDP 端口参数：

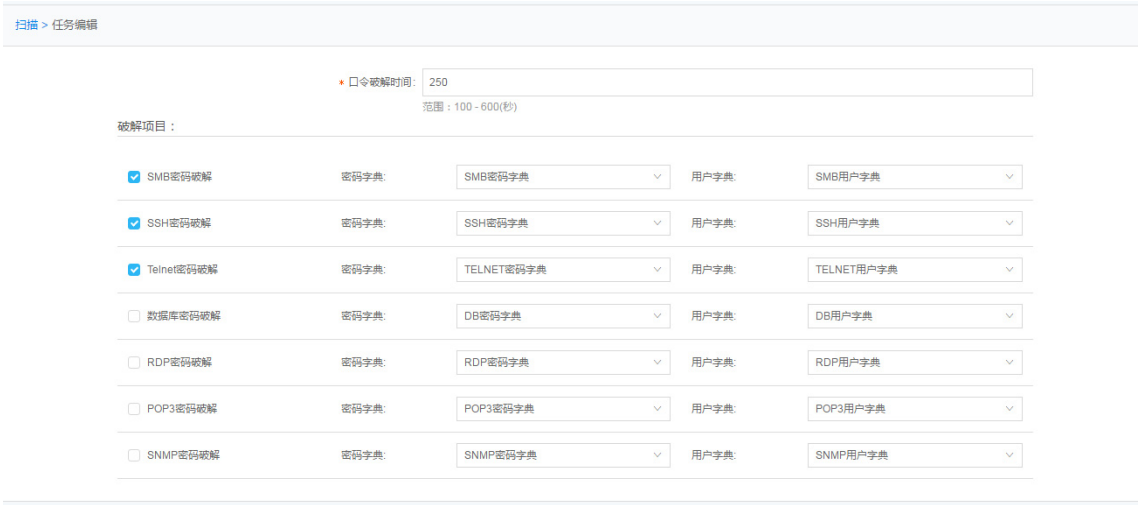
- <端口扫描速度>：系统对远程主机发送 UDP 数据包的速度及大小，可选参数包括“较快”，“普通”和“较慢”，扫描速度越慢，获取的端口开放信息越准确，耗时也会比较长。系统缺省选项为“普通”。
- <扫描范围设置>：支持典型端口、特殊端口、全部端口、自定义端口的设置。选中【典型端口】只扫描一些常用的端口（可在【模板】>【数据字典】>【所有字典】>【端口字典】中查看）；选中<特殊端口>时扫描的端口范围是 1-1024；选择<全部端口>则扫描的端口范围 1－65535；选中<不扫描>则不对 UDP 端口进行扫描；<自定义端口>可根据用户需要定义要扫描的 TCP 端口。

3. 破解参数

功能描述：口令破解时间、协议方式及对应的用户名字典与密码字典配置。

配置路径：【扫描】>【新增任务】>【主机扫描参数】>【破解参数】，如下图所示。

图3-24 主机扫描参数-破解参数配



参数说明：

- <口令破解时间>：扫描过程中进行密码破解尝试的时间，可行时间范围从 100－600 秒，系统缺省值为 250 秒。
- <破解项目>：选择要破解的协议与用来进行密码破解所使用的用户和密码字典。勾选指启用相应的协议密码破解，通过下拉菜单选择相应的用户名字典与密码字典。

3.1.3 Web扫描参数

功能描述：Web 扫描选项、Web 检测、扫描登录设置的配置。

配置路径：【扫描】>【新增任务】>【Web 扫描参数】

1. 配置扫描选项

功能描述：扫描范围、Web 访问、Web 爬行、链接过滤、流量限制、Web2.0、表单的配置。

配置路径：【扫描】>【新增任务】>【Web 扫描参数】

(1) 常规

图3-25 Web 扫描参数-常规

参数说明：

- <站点扫描顺序>：支持同时扫描和顺序扫描。
- <扫描模式>：支持边爬行边扫描、先爬行后扫描、只爬行、只检测。

(2) 扫描范围

图3-26 Web 扫描参数-扫描范围

参数说明：

- <扫描目录范围>：扫描目录范围包括：扫描当前域、扫描整个域、检测当前页、仅扫描目录 url 下的链接、扫描所有链接。
- <其他服务和域>：在扫描中包含其他服务器和域。
- <最大 URL 链接限制>：设置扫描的最大 URL 链接数，在达到该链接数后停止扫描，-1 表示不限制 URL 链接数量。设置具体的个数如 10000，当爬行到 10000 个 URL 时，系统会停止爬行。默认设置为-1。

(3) Web 访问

图3-27 Web 扫描参数-Web 访问

参数说明：

- <HTTP 协议版本>：HTTP 协议版本号，用户可以根据需要选择 HTTP1.1 或 HTTP1.0 不同版本协议，默认设置为自动。

- <操作系统类型>：指定操作系统类型，扫描器将扫描相关操作系统的漏洞。
- <Web 服务器类型>：支持 Web 服务器类型的判断，默认配置为自动判断。
- <连接服务器超时（秒）>：主应用程序发出 HTTP 请求到接收服务端接收响应时间，默认 15 秒，用户可以自行修改，建议使用默认配置。
- <HTTP 传输超时（秒）>：HTTP 传输超时时间设置，默认传输超时时间为 30 秒。
- <HTTP 请求失败重试次数>：主应用程序向服务端发送 HTTP 请求失败（服务器没有响应请求或传输超时）后，再次重新发送相同的请求的次数。默认设置 3 次。
- <HTTP 支持语言>：可以选择中文(zh-cn)和英文(en-us)，默认设置中文(zh-cn)。
- <User-Agent 文本>：用户代理文本，即访问的浏览器文本信息，它是一个特殊字符串头，使得服务器能够识别客户使用的操作系统及版本、CPU 类型、浏览器及版本、浏览器渲染引擎、浏览器语言、浏览器插件等。
- <每个页面最大接收内容长度（字节）>：表示引擎每个页面最大接收的内容长度，默认设置 1048576 字节。

(4) Web 爬行

图3-28 Web 扫描参数-Web 爬行

参数说明：

- <如果首页跳转，同时扫描新域名>：是否支持首页跳转。若选择<是>则支持首页跳转并扫描新域名。选择<否>则不支持首页跳转，只扫描当前域名。
- <路径模式排重>：在扫描过程中爬到路径类似的链接是否需要排重。若选中<是>，表示排重，不会扫描，否则扫描。

提示

- 路径模式排重指当 URL 的路径部分出现数字时，如果 2 个 url 的路径除了数字以外都一样，则只保存和检测其中一个 URL。
- 这种方式的排重目的是提高效率。例如以下 URL 选择了“是”则会排重，只会爬行一个 URL。
- 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

- <参数排重>：支持无、按参数名排重、按参数组合模式排重三种参数排重方式。

提示

1、按参数名排重。

- 参数无顺序的，只要参数一样就排重。
- 例如 http://192.168.23.5/web/product.asp?tp=67。这个 URL 中的 tp 就是一个参数。随着 tp 的值的变化可能会有多个 URL 链接。按参数名排重的意思是只爬行 tp 参数的一个值，其他的不爬行，如爬行了 tp=67，那么 tp=68 或其他的值就不会爬行了。爬取多少个 URL 后开始排重由“同参数 URL 数量”选项指定

2、按参数组合模式排重。

- 参数有顺序，只有顺序一致才排重。
- 例如 http://192.168.23.5/web/login.asp?para1=参数 1&para2=参数 2&para3=参数 3。此链接参数名称按数学排列组合，最多爬行 6 个。爬取多少个 URL 开始排重由“同参数 URL 数量”选项指定。

3、无：表示所有的 URL 都进行爬行。

- http://www.**.com/news/2010-12-03/2.html

- <同参数 URL 数量>：参数名相同，参数值不同的 URL 保留数量，此配置项有效的前提是【参数排重】不为无。
- <同一路径最大 URL 数量>：静态 url，同一路径下且最后一级都是数字的，保存的 url 的数量。如 http://192.168.23.5/web/11.html。
- <相近格式 URL 爬行数量>：限制格式相近的 URL 爬行的数量，默认为 0，表示不限制爬行数量。
- <爬行层数限制>：限制爬虫向下爬行层数，默认为 0，表示不限制爬行层数。
- <爬行路径深度限制>：限制爬虫爬行的路径深度，默认为 10。

- <每个目录的最大子目录和文件个数>：设置每个目录爬行的最大子目录和文件数，默认为512。
- <路径区分大小写>：开启时当路径含有相同字母时区分为不同链接。
- <参数区分大小写>：开启时当参数含有相同字母时区分为不同链接。
- <是否启用路径字典探测>：开启时启用路径字典探测功能。
- <路径字典探测最大深度>：设置路径字典探测最大目录深度。
- <是否启用路径字典探测协程>：设置是否支持多线程进行路径字典探测。
- <路径字典探测线程数量>：路径字典探测线程数量，开启协程时用；开启协程时，默认是 3 个线程，最大 30，最小 0 则不开启线程。
- <路径字典探测一个协程处理的字典数量>：路径字典探测一个协程处理的字典数量，开启协程时用；开启协程时，默认是 1 个协程处理 50 个 url，最大 600，最小 5。

(5) 链接过滤。

图3-29 Web 扫描参数-链接过滤

参数说明：

- <保存文件类型白名单>>：后缀名在白名单中的 URL 地址会被保存。
- <爬行文件类型白名单>：爬行网站过程中有很多类型脚本、页面文件类型，只对设置在白名单中的类型文件进行爬行和检测。
- <检测文件类型白名单>：检测网站过程中有很多类型脚本、页面文件类型，只对设置在白名单中的类型文件进行检测。
- <不爬行的文件类型>：用于配置扫描时不爬行的文件类型，从爬行中排除这些类型的文件，例如 mp3、rar。
- <不检测的文件类型>：用于配置扫描时不抓取的文件类型，默认不扫描以下几种文件类型：3dm,bmp,gif,ico,jpf,jpg,jpeg,pct,pcx,png,ps,psd,psp,thm,tif,tiff,wmf,css,js。
- <不自动扫描的域名>：当扫描时遇到这些域名则不执行扫描。默认遇到以下域名时不执行扫描：*.g.cn,*.google.*,*.yahoo.*,*.baidu.*,*.sina.*,*.sohu.*,*.taobao.*,*.alipay.*,*.qq.*,*.360.*
- <注销页面检测>：包含以下任何一个字符串的页面为注销页面，不进行扫描，例如 logout、off、signout、logoff、signoff、exit、quit、bye-bye、clearuser、invalidate。
- <只扫描匹配的页面>：检测网站过程中，只扫描添加到该列表中的页面，添加到列表中的参数支持通配符。如在列表中添加*cms*,在爬行网站时只会爬行匹配到含有 cms 的页面。
- <只扫描指定目录下的页面>：仅扫描指定目录下面的 url,例如/dir3/dir4,多个用逗号隔开。
- <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，例如：注销，若有多个则用逗号隔开，默认忽略含有页数关键字的链接，例如 delete、logoff、exit 等。
- <跳过所有表单>：默认为否。如果设置为是，在扫描过程中，将跳过所有的表单。
- <跳过登录表单>：默认为否。如果设置为是，在扫描过程中，将跳过所有的登录表单。
- <目录黑名单>：存在于黑名单中的目录将不被扫描,只有在目录白名单为空时黑名单才有效,配置格式例如/dir3/dir4。
- <动态页面的后缀列表>：根据 url 的后缀来判断是否是动态页面,例如 asp、jsp、php。
- <静态页面的后缀列表>：根据 url 的后缀来判断是否是静态页面,例如 html、htm。

图3-30 Web 扫描参数-流量限制

- <最低限速>：设置最低限速，若访问速度低于最低速度则会终止访问，-1 表示不限制最低速度。
- <每秒最大发送发送请求数>：表示引擎每秒最大发送请求个数，默认配置为 256。
- <系统休眠时间>：配合每秒发送请求个数用，当发送完设置的每秒请求个数的时间不足 1 秒，程序就休眠一下，休眠时间的单位为毫秒，默认配置为 1。
- <最大收发速率（千字节/秒>：限制最大发包速率，默认值-1 表示不限制收发速率。
- <允许的访问 http 请求的最大连接数量>：设置保存已创建的连接数量，以备重用，用于提高数据通信速率，默认最大连接数为 5。
- <扫描倍速>：同一时刻允许并行扫描的 URL 数量，-1 表示不作限制。

图3-31 Web 扫描参数-Web2.0

参数说明：

- <开启模拟点击按钮功能>：用于模拟用户鼠标点击事件。
- <执行 JavaScript 脚本>：执行 JavaScript 脚本选择“是”时会启用动态爬虫，选择“否”时则不启用动态爬虫。
- <执行 JavaScript 脚本进程数>：执行 JavaScript 脚本进程数，默认是 1 个，最大 3。
- <执行 js 脚本的 User-Agent 文本>：执行动态爬虫时默认的浏览器
- <执行 js 脚本网页渲染时间>：表示渲染网页等待的时间，单位毫秒，某些含有 ajax 的 url 的等待渲染完成的时间
- <深度解析>：是否支持对网站内容进行深度解析，默认为否。
- <深度解析渲染时间>：表示渲染网页等待的时间，单位毫秒，某些含有 ajax 的 url 的等待渲染完成的时间。
- <解析 Flash 文件中的 URL>：引擎会解析 Flash 文件中包含的 URL，默认设置“是”。

图3-32 Web 扫描参数-表单

参数说明：

- <自动填充表单>：系统对于表单包含 GET 和 POST 操作会自动解析提取进行检测，用户可以对特定字段填充自己的值，如希望添加自己的用户名，可设置*username*=u，并将此设置填在最前面。

提示

- 参照设置如下。
- addr*=newroad,*age*=24,*area*=0571,*city*=HangZhou,*day*=01,*month*=01,*year*=2016,*=1，当检测表单匹配到包含 addr 等字符字段参数时，会自动填充。否则用 1 填充。

- <对包含 textarea 元素的表单进行测试>：选择是否对包含 textarea 元素的表单进行测试。

2. Web检测

功能描述：常规检测。

配置路径：【扫描】>【新增任务】>【Web 扫描参数】>【Web 检测】

图3-33 Web 扫描参数-Web 检测

参数说明：

- <名称相同的参数不重复检测>：选择“是”后系统对名称相同的参数不进行重复检测。
- <自定义 404url>：添加自定义 404 的 url 列表。
- <自定义 404 页面包含字符串>：添加自定义 404 的字符串列表
- <不检测的参数>：URL 带的参数如果属于不检测的参数，则不会对此参数进行检测，支持多个不需要检测的参数。
- <敏感词汇>：敏感词汇列表，对敏感词检测时使用。
- <攻击有效载荷（payload）大小写随机>：在攻击是可选择是否随机大小写 payload，默认为否。
- <url 空格替换方式>：选择使用哪种编码空格,编码只针对 sql 注入漏洞和跨站脚本攻击漏洞。
- <检测深度>:允许检测的 url 最大深度,0 及以下表示不限制,这条配置只针对木马类型的检测。
- <url 编码方式>：选择 url 的编码方式,编码只针对 sql 注入漏洞和跨站脚本攻击漏洞。
- <url 编码字符选择>：在上一条选择参数值或者整个检测参数编码后，这个配置才起作用，这里的编码方式对空格无效。

3. 扫描登录设置

功能描述：提供 Web 认证、页面登录、代理设置功能。

配置路径：【扫描】>【新增任务】>【Web 扫描参数】>【扫描登录设置】

图3-34 Web 扫描参数-Web 认证

参数说明：

- <认证方法>：认证方法支持无、自动（除 basic 之外）、Basic、Digest、Digest 认证(IE 风格)、NTLM。
- <用户>：用户根据情况选择认证方法后，输入 httpAuth 认证的用户名。
- <密码>：用户根据情况选择认证方法后，输入 httpAuth 认证的密码。
- <SSL 版本>：选择相应 SSL 版本。

(1) 页面登录

图3-35 Web 扫描参数-页面登录

参数说明：

- <登录 URL>：设置登录页面的 URL。
- <用户名参数>：识别可能是用户名的参数。
- <密码参数>：识别可能是密码的参数。
- <用户名>：登录账号
- <密码>：登录密码

(2) 代理设置

图3-36 Web 扫描参数-代理设置

参数说明：

- <代理服务器类型>：代理服务器类型主要包含不使用代理、HTTP 代理、Sockets 代理。
  - 不使用代理：直接扫描被测网站。
  - HTTP 代理：设置 HTTP 服务器 IP 和端口，1080 是默认端口，用户可以根据 HTTP 代理服务器的端口进行修改。对于身份认证验证的代理服务器，可以在下方设置代理服务器用户名和密码。
  - Sockets 代理：设置方式同 HTTP 代理，只是扫描器与代理服务器之间通信协议不同而已。

3.1.4 数据库扫描参数

功能描述：提供常规参数、端口参数、破解参数等扫描参数配置。

配置路径：【扫描】>【新增任务】>【数据库扫描参数】

1. 常规参数

功能描述：提供扫描线程数、允许同时扫描主机数、扫描方式、漏洞扫描参数等扫描参数的配置。

配置路径：【扫描】>【新增任务】>【数据库扫描参数】>【常规参数】，配置界面如下图所示。

图3-37 数据库扫描参数-常规参数配置

参数说明：

- <扫描进程数>：系统进行漏洞扫描时，扫描引擎将启动的最大扫描并发进程数量。扫描进程数与所需的系统资源数成正比，扫描进程数越大，扫描效率越高，其所需的系统资源也就越多。但并非扫描进程数越大越好，到达一定数目后增加进程数对扫描速度的提高作用有限，反而浪费系统资源。此参数的允许范围和默认优化值因产品型号不同而不同。
- <允许同时扫描主机数>：系统最大主机扫描并发数量。允许并发扫描主机数越多，系统的扫描效率越高，但主机数到达一定数目后，将增加系统的负荷，系统效率提高有限。此参数的允许范围和默认优化值因产品型号不同而不同。
- <脚本检测超时时间>：是指单个漏洞脚本的执行时间若超过“脚本检测超时时间”则会停止对该漏洞项的扫描，以加快扫描速度。该参数默认优化值为“60 秒”。
- <在线判断超时时间>：是指系统判断远程主机是否在线的时间阀值，系统在“在线判断超时日间”值内，未收到远程主机的响应，则判断远程主机不在线。
- <扫描方式>中的<强制扫描>指扫描引擎将不判断目标主机是否在线而直接对其进行漏洞扫描。若在<强制扫描>参数选项中选“否”，则系统在扫描时将先判断目标主机是否在线，若不在线则不对该主机进行扫描。此参数默认优化值为“否”。

- <报告级别>包含“精确”、“常规”、“全面”三个选项，其中“精确”，报告中仅包含根据漏洞原理识别风险的漏洞；“常规”，报告中排除根据据版本号识别风险外的所有漏洞；“全面”，报告中包含所有可能存在风险的漏洞；
- <调试模式>应用场景，用于原厂商工程师非现场情况下收集客户环境下脚本的调试信息，协助客户完成漏洞测试和确认。此参数默认优化值为“关闭”。
- <在线检测方法>指检测远程主机是否线的方法，包括 ICMP 和 ICMP+CONNECT 两种检测方法。ICMP 通过发送 ICMP 包给远程主机，ICMP+CONNECT 除了通过发送 ICMP 包外，还可通过 TCP 连接状态来判断远程主机是否在线，TCP 端口号通过逗号（,）隔开。
- <安全扫描>指系统在扫描远程主机漏洞的时候，不会对远程主机造成伤害的扫描方式。此参数默认优化值为“是”。

2. 端口参数

功能描述：包含 TCP 端口参数的配置。

配置路径：【扫描】>【新增任务】>【数据库扫描参数】>【端口参数】，如下图所示。

图3-38 数据库扫描参数-端口参数配置

参数说明：

- <扫描超时时间>：单个脚本的扫描超时时间，若等待超过设置的时间则系统会停止对该漏洞项的扫描，以加快扫描速度，超时时间可配置范围为 100 到 5000 毫秒，系统缺省值为 300 毫秒。
- <扫描范围设置>：支持典型端口、特殊端口、全部端口、自定义端口的设置，选中【典型端口】只扫描一些常用的端口（可在【模板】>【数据字典】>【所有字典】>【端口字典】中查看）；选择【特殊端口】时扫描的端口范围是 1-1024；选择【全部端口】则扫描的端口范围为 1－65535；选中“不扫描”则不对 TCP 端口进行扫描；选中“自定义端口”后，用户可根据需要定义要扫描的 TCP 端口。
- <扫描方式设置>：扫描 TCP 端口时采用的扫描方式，包括 tcpconnect 和 tcpsync 两种扫描方式，其中 tcpconnect 通过 TCP 连接状态来判断远程主机是否有开放相应的 TCP 端口；tpcsync 通过是 TCP/IP 建立连接时使用的三次握手的状态来判断远程主机是否有开放相应的端口。

3. 破解参数

功能描述：口令破解时间、协议方式及对应的用户名字典与密码字典配置。

配置路径：【扫描】>【新增任务】>【主机扫描参数】>【破解参数】，如下图所示。

图3-39 数据库扫描参数-破解参数配置

参数说明：

- <口令破解时间>：扫描过程中进行密码破解尝试的时间，可行时间范围从 100－600 秒，系统缺省值为 250 秒。
- <破解项目>：选择要破解的协议与用来进行密码破解所使用的用户和密码字典。勾选指启用相应的协议密码破解，通过下拉菜单选择相应的用户名字典与密码字典。

提示

密码破解，可能导致数据库被锁死。

3.1.5 主机通知参数

1. 扫描通知

功能描述：创建扫描任务时，对任务开始及结束时是否发送相关消息通知管理员及相关参数的配置。

配置路径：【扫描】>【新增任务】>【主机通知参数】>【扫描通知】，如下图所示。

图3-40 主机通知参数-扫描通知

参数说明：

- <扫描预通知>：系统开始扫描时，是否向目标主机发送扫描开始的消息通知。
- <结束通知>：支持消息通知及邮件通知两种方式。开启消息通知，扫描结束后，可向目标主机发送扫描结束的消息通知；开启邮件通知并设置邮箱地址，则扫描任务结束后，将发送邮件到指定的邮箱通知用户扫描任务已结束。

提示

- 关于消息通知和邮件通知的前提如下。
- 消息通知：开启了消息服务的目标主机才能收到提示。
- 邮件通知：需要在系统管理的 SMTP 设置中进行发送邮箱设置，同时目标主机必须是对象管理中的对象并设置了用户 E-Mail 地址。

2. WSUS通知

功能描述：创建扫描任时对扫描结果发现漏洞的主机，是否自动指向 windows 补丁升级服务器修复补丁。

配置路径：【扫描】>【新增任务】>【通知参数】>【WSUS 通知】如下图所示。

图3-41 主机通知参数-WSUS 通知

参数说明：

- <启用>：启用 WSUS 服务器
- <WSUS 地址>：设置 WSUS 服务器的地址。WSUS 压缩包发送至当前登录用户邮箱，WSUS 压缩包包含 wsus.reg 文件。
- <安装方式>：配置补丁安装时，是否要提醒管理员。系统缺省配置为不提醒管理员，直接更新补丁。

提示

WSUS 是 Windows Server Update Services 的简称，即 Windows Server 更新服务。通过 WSUS 服务器，所有的 Windows 更新都集中下载到内网的 WSUS 服务器中，而内网中的目标主机可通过 WSUS 服务器来更新补丁。这在很大程度上节省了网络资源，避免了外部网络流量的浪费并且提高了内部网络中计算机更新的效率。

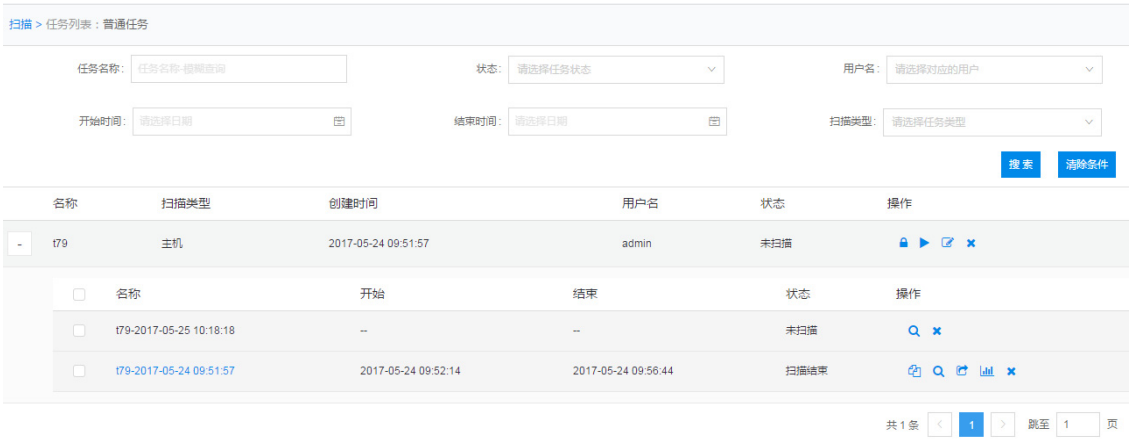
3.2 任务管理

3.2.1 普通任务

功能描述：新建普通任务，任务列表生成一条任务记录，此任务记录包含主任务和子任务，每次重新扫描会生成一个子任务；主任务对应的功能包括：锁定/解锁、重新扫描、暂停扫描、继续扫描、停止扫描、编辑、删除，子任务对应的功能包括：复制、查看任务配置、导出任务、报表生成、删除、对比分析。

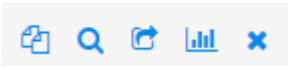
配置路径：【扫描】>【普通任务】如下图所示。

图3-42 扫描任务列表



参数说明：

- <搜索>：支持不同条件对扫描任务进行搜索，搜索条件支持：任务名称、状态、用户名、时间段、扫描类型。
- <扫描结果查看>：点击子任务名称可以查看扫描详情，按主机、漏洞、服务、账户分类显示相应的信息。用户可以在该页面上看到目标主机的基本信息、主机信息、服务信息和漏洞信息等。
- <操作列>：以图标形式展示可对扫描任务进行的操作，主任务与子任务对应的操作不同：
  - 正在扫描的任务，主任务对应的操作为  ，从左到右图标依次是【锁定】、【暂停扫描】、【停止扫描】，子任务对应的操作为  ，该图标为【查看任务配置】。
  - 已暂停的任务，主任务对应的操作为  ，从左到右图标依次是【锁定】、【继续扫描】、【删除】，子任务对应的操作为  ，从左到右图标依次是【复制】、【查看任务配置】、【报告】、【删除】；点击主任务的  ，被暂停的子任务开始接着扫描。

- 已停止或扫描结束的任务，主任务对应的操作为  ，从左到右图标依次是【锁定】、【重新扫描】、【编辑】、【删除】；子任务对应的操作为  ，从左到右图标依次是【复制】、【查看任务配置】、【导出】、【报告】、【删除】，点击  复制该任务创建一条新的任务（包含主任务和子任务）；点击  指根据不同角色需要、不同的报表模板生成相应的扫描报告并下载到本地；点击  看删除当前的扫描任务。
- 已锁定的任务，主任务对应的操作为解锁  ，子任务对应的操作按钮被屏蔽。

1. 复制任务

点击子任务“操作”栏目下的  可以对子任务进行复制，复制的任务不允许重名，复制成功后生成一条新的任务，该任务包含主任务和子任务。具体复制流程可以参考 2.1 新增任务。

2. 导出任务

选择扫描子任务，点击  ，任务文件下载到本地保存。

3. 导入任务

点击  ，上传导出的任务文件，支持批量导入，导入成功后在任务列表。

4. 查看任务配置

点击子任务“操作”栏目下的  可以对任务进行查看，查看状态下，任务配置不允许被修改。

5. 编辑任务

点击子任务“操作”栏目下的  可以对任务进行编辑，任务名称、扫描类型、扫描目标不允许编辑

6. 锁定任务

选中未加锁扫描任务，点击  ，输入正确密码进行加锁。

7. 解锁任务

选中已加锁扫描任务，用户点击  ，输入正确密码进行解锁。

8. 生成报表

点击“操作”栏目下的  ，弹出如下界面。

图3-43 报表下载

参数说明：

- <报表类型>：选择导出的报表类型，主机和数据库扫描任务对应的报表类型有 html 报表，word 报表，xml 报表以及 pdf 报表四种种格式；而 web 扫描任务对应的报表类型有 html、word、pdf、xml、csv、excel 六种格式。
- <报表模板>：主机和数据库扫描任务对应的默认模板有 3 种，分别是技术工程师、安全工程师、行政主管；web 扫描任务对应的默认模板有 7 种，分别是技术工程师、安全工程师、行政主管、OWASP TOP10 2013 版、等级保护报表 2 级、等级保护报表 3 级、等级保护报表 4 级；不同的报表模板展示内容有所不同，此功能可在【模板】>【报表模板】>设定。具体设置见 3.3 报表模板说明。
- <确定>：点击<确定>后，系统会将扫描结果根据设定的报表类型和报表模板生成相应的报告并下载到本地。

提示

若报告无法正常导出，请注意查看浏览器右上角，下载文件是否被浏览器拦截，若是被拦截若是被拦截则选择放行，即可正常下载则选择放行，即可正常下载。

9. 删除任务

点击“操作”状态下的 即可删除对应的任务，删除任务有二次确认提示，请确认是否进行删除。

提示

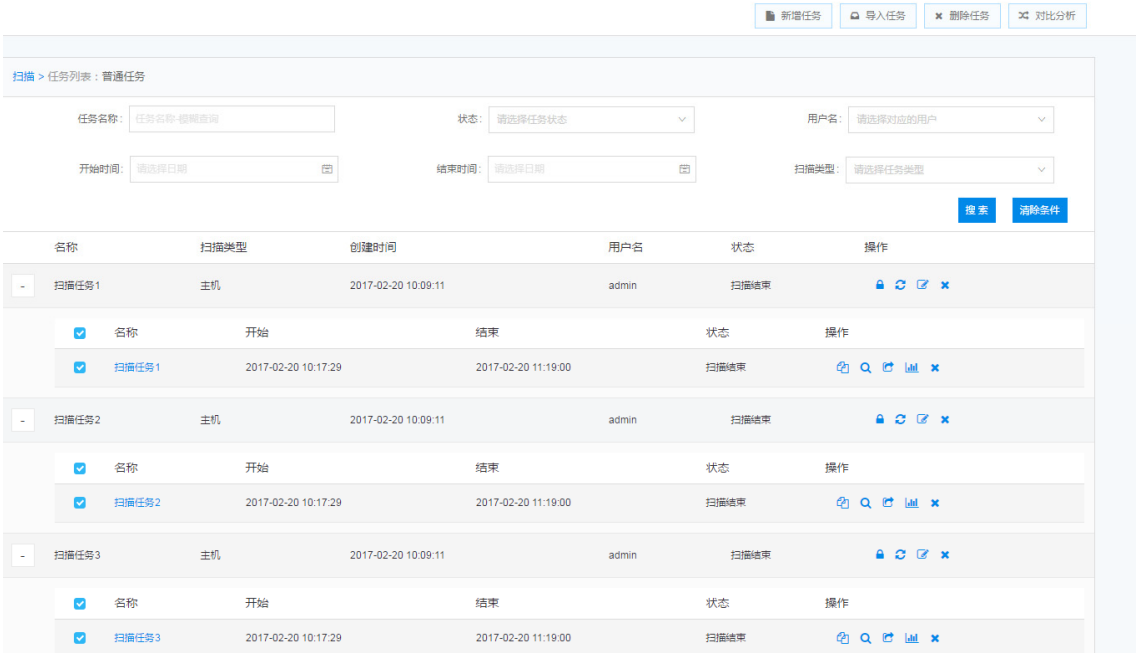
在无备份数据的情况下，删除是不可逆操作。

10. 对比分析

功能描述：是对同一目标相同策略情况下不同时间的扫描结果的对比，对比方式包括：任务对比、主机对比，URL 对比，数据库主机对比，以图表方式直观和清晰地对同一目标在不同时间扫描的漏洞数量的变化，支持对比分析报告的导出。

配置路径：【扫描】>【普通任务】>【对比分析】如下图所示。

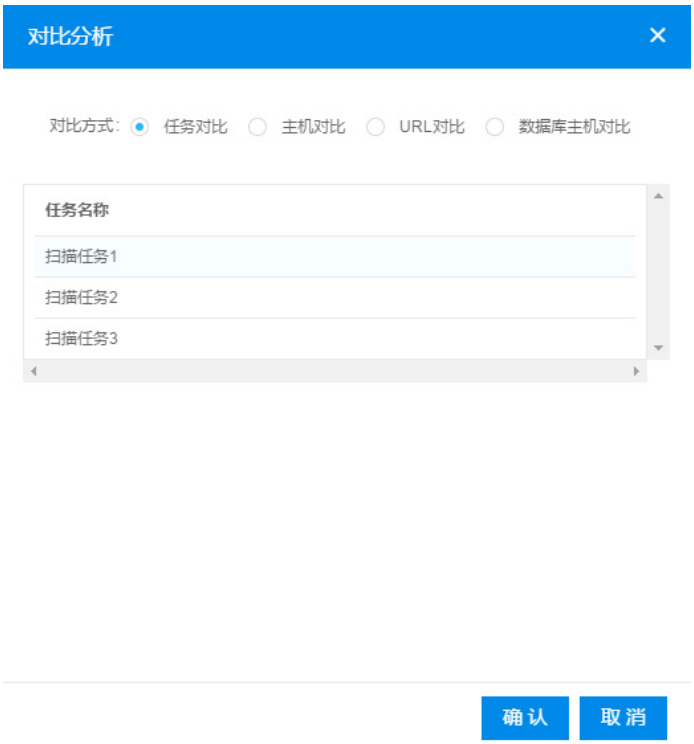
图3-44 扫描任务对比



选中 2~5 个同一目标的扫描任务，点击右上角的 

，弹出如下界面。

图3-45 对比分析



参数说明：

- <对比方式>：对比方式支持任务对比、主机对比、URL 对比、数据库主机对比，根据对比对象的不同，展示的分析结果会所有不同，各有侧重。点击<确认>开始进行同一目标不同扫描任务的对比分析，以任务对比为例，对比分析结果如下。

图3-46 任务对比分析报告

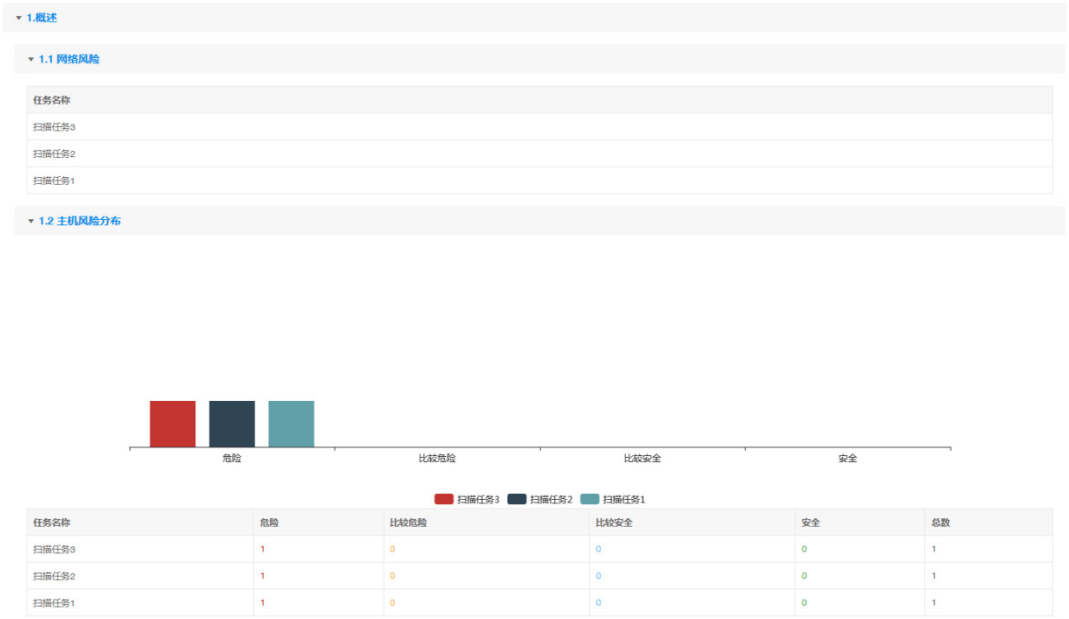


图3-47 任务对比分析报告

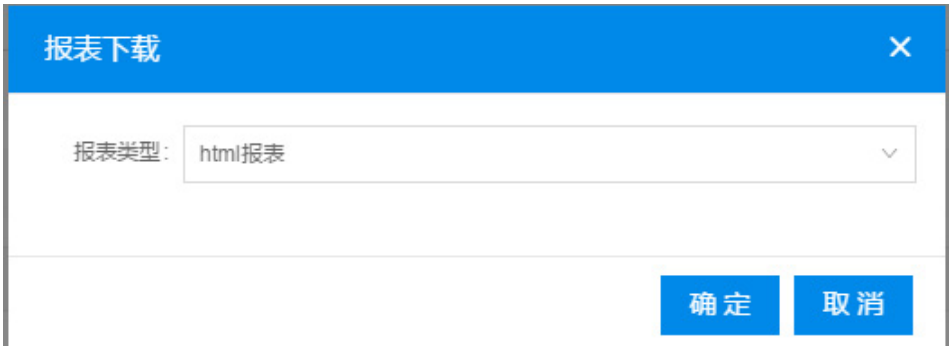
扫描任务对比分析报告给出了选定的几个扫描任务的总漏洞数、紧急风险漏洞数、高风险漏洞数、中风险漏洞数、低风险漏洞数和信息数的对比分析，并以图表的形式直观地给出漏洞数的对比情况。用户可以很清晰地看出几个扫描任务的差异；对比分析报表支持导出到本地。

在对比分析任务选择页面上选择<主机对比>，即可进入到主机对比分析页面，页面上列出所选的扫描任务扫描到的所有主机 IP 相同的扫描任务。所扫描到的选定各主机的总漏洞数、紧急风险漏洞数、高风险漏洞数、中风险漏洞数、低风险漏洞数和信息数的对比分析，并以图表的形式直观地给出漏洞数的对比情况。用户可以很清晰地看出每台主机在不同的扫描任务中扫描漏洞数的差异。

点击右上角栏目的 

，弹出如下界面。

图3-48 报表下载



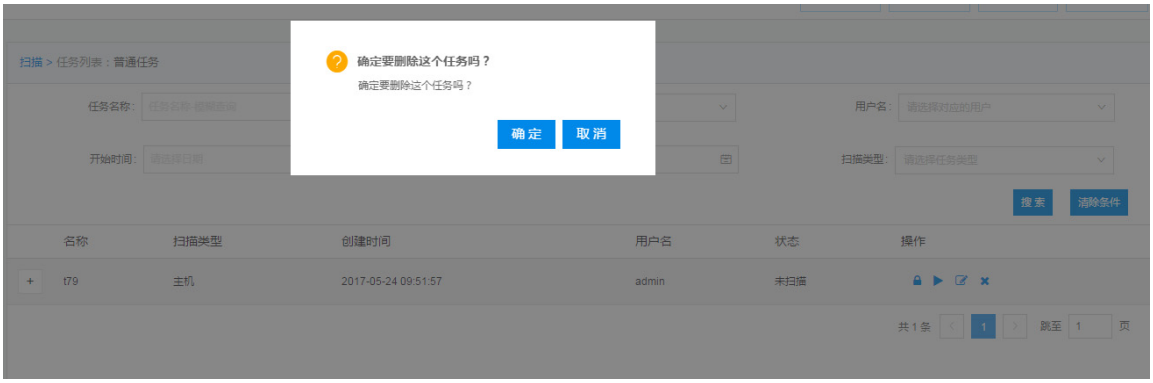
- <报表类型>：选择导出的报表类型，对应的报表类型有 html 报表，word 报表以及 pdf 报表三种格式。

11. 任务删除

功能描述：删除扫描任务。

配置路径：【扫描】>【普通任务】>【任务删除】如下图所示。

图3-49 任务删除



点击<确定>即可删除相应的扫描任务。

12. 计划任务

功能描述：查看周期性执行的扫描任务状态，系统可以根据用户创建的计划任务在指定的时间自动启动扫描引擎对设定的扫描目标进行扫描。

配置路径：【扫描】>【计划任务】如下图所示。

图3-50 计划任务列表

参数说明：

- <取消定时任务>：点击 ，取消定时任务，到设定的时间就不会自动启动扫描任务。
- <查看定时任务配置>：点击 ，可查看定时任务配置详情。
- <编辑任务>点击子任务“操作”栏目下的 可以对任务进行编辑，任务名称、扫描类型、扫描目标、不允许编辑。
- <删除定时任务>：点击 ，可删除定时任务，删除后列表中不存在该记录。

4 模板

4.1 策略模板

功能描述：用于配置主机扫描、数据库扫描以及 Web 扫描策略模板，用户可以在该模块下自定义扫描策略。

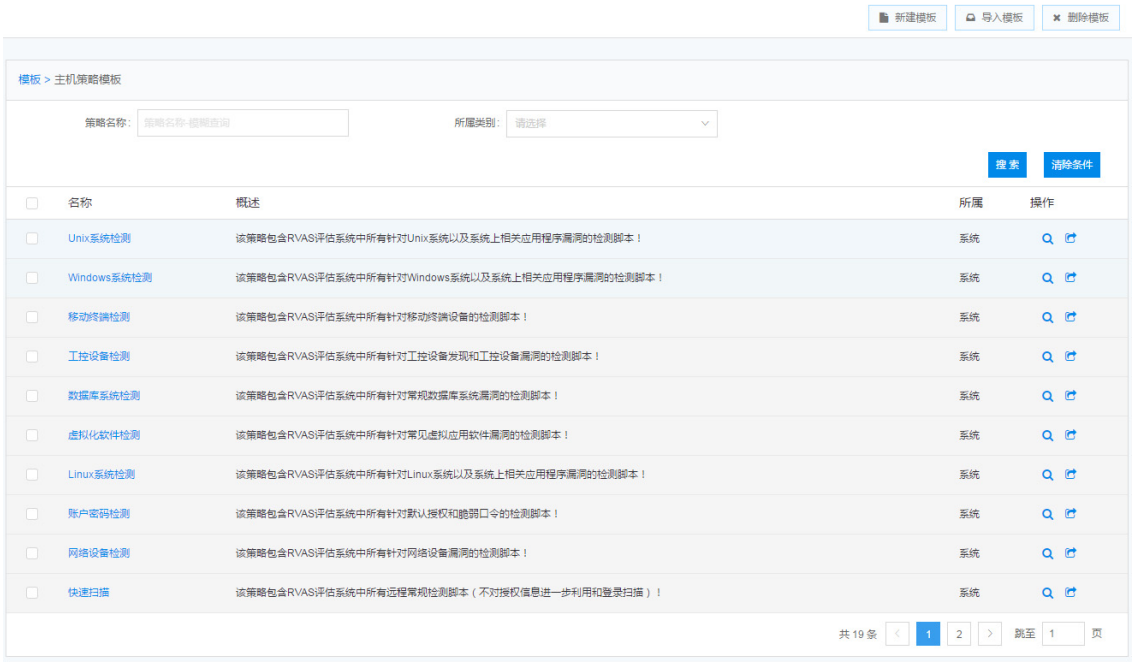
配置路径：【模板】>【策略模板】

4.1.1 主机扫描策略模板

功能描述：用于配置主机扫描策略模板，用户可以在该模块下自定义扫描策略。

配置路径：【模板】>【策略模板】>【主机策略模板】，界面如下图。

图4-1 主机扫描策略模板



参数说明：

- <搜索>：可对策略模板进行搜索，支持按策略名称、所属类别进行搜索。
- <清除条件>：将输入的搜索条件清空。
- <查看>：点击，可查看模板详情。
- <导出>：点击，可将策略模板下载到本地作为备份，下载的文件格式为 xml。
- <新建模板>：点击 新建模板，跳转到新建策略模板的界面，用户可根据扫描目标自定义模板，达到针对性扫描的目的。

- <导入模板>：导入策略模板，前提是已将相应的策略模板导出到本地。
- <编辑模板>：点击 ，可修改自定义的策略模板。
- <删除模板>：点击 或选中模板，点击 删除模板 ，可删除用户创建的策略模板。

说明

系统默认的主机策略模板不能进行修改、删除操作。

---

1. 模板查询

功能描述：用于查询符合条件的模板。

配置路径：【模板】>【策略模板】如下图所示。

图4-2 主机扫描策略模板-查询

参数说明：

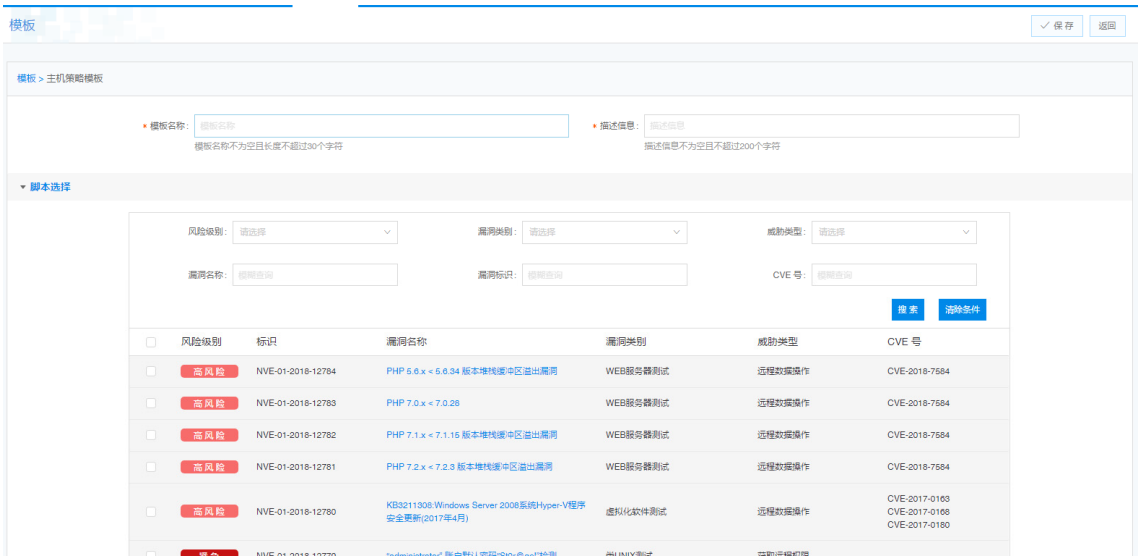
- <策略名称>：在在该项中输入相应的名称，即可查询到相应的模板，若是无查询的模板数据，则会提示暂无数据。
- <所属类别>：所属类别有 2 种，分别是“系统”和“用户”。系统自带的模板即为系统模板，系统模板无法进行修改与删除操作。用户建立的模板类别为“用户”，可以进行修改删除操作。

2. 新建模板

功能描述：用户可根据扫描目标自定义主机扫描策略模板，达到针对性扫描的目的。

配置路径：【模板】>【策略模板】>【主机扫描策略模板】>【新建模板】

图4-3 主机策略模板-新建



参数说明：

- <模板名称>：输入模板名称。
- <描述信息>：为新建的模板设定描述信息。
- <搜索>：支持按风险级别、漏洞类别、威胁类型、漏洞名称、漏洞标识、CVE 号查询脚本。
- <脚本选择>：默认展示系统内置的主机扫描策略，通过勾选/取消勾选脚本来配置模板。
- <保存>：配置完成点击<保存>完成主机扫描策略模板的新建。
- <返回>：点击<返回>则取消新建或修改模板操作。

3. 导入模板

功能描述：导入主机扫描策略模板。

配置路径：【模板】>【策略模板】>【主机扫描策略模板】>【导入模板】如下图所示。

图4-4 主机扫描策略模板-导入策略模板

导入策略模板的前提要将相应的策略模板导出。先输入模板名称，点击<选择文件>打开文件选择框，先为导入的模板进行命名。选择要导入的策略模板文件或拖动要导入的文件至导入区域。点击<确定>，将已选择的文件中的策略模板导入漏洞扫描系统。

提示

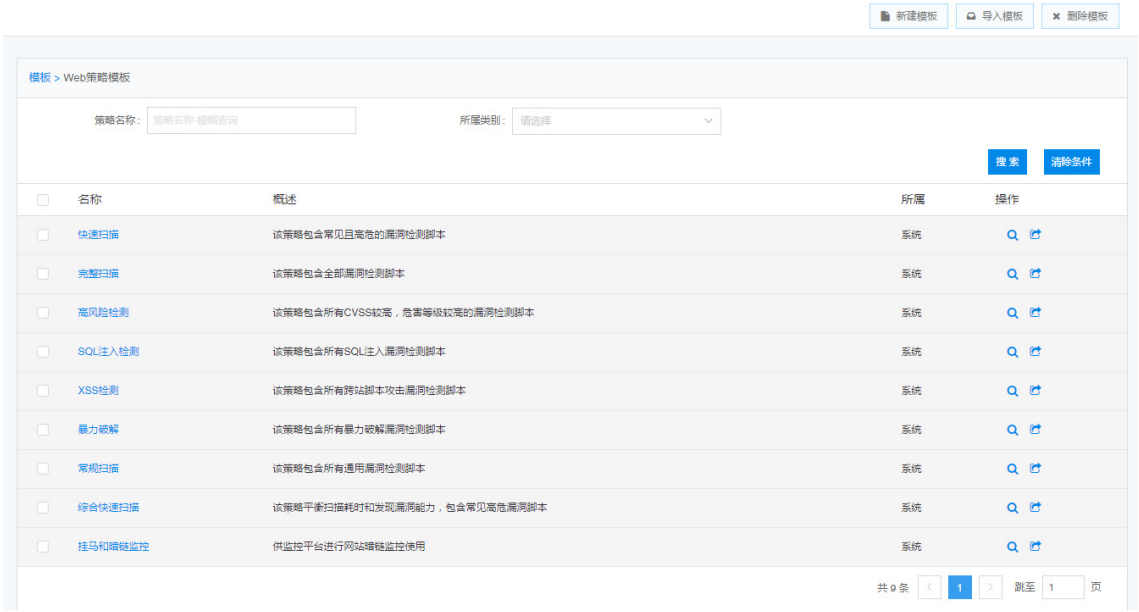
- 导入策略模板的前提是已将相应的策略模板导出并下载到本地磁盘。
- 若模板名与已有的模板重名，或未填写模板名称名，会出现修改或者填写模板名的提示。

4.1.2 Web策略模板

功能描述：用于配置 Web 策略模板，用户可以在该模块下自定义 Web 扫描策略。

配置路径：【模板】>【策略模板】>【Web 策略模板】，界面如下图。

图4-5 Web 策略模板



参数说明：

- <搜索>：可对策略模板进行搜索，支持按策略名称、所属类别进行搜索。
- <清除条件>：将输入的搜索条件清空。
- <查看>：点击，可查看 Web 策略模板详情。
- <导出>：点击，可将 web 策略模板下载到本地作为备份，下载的文件格式为 xml。
- <新建模板>：点击 新建模板，跳转到新建策略模板的界面，用户可根据扫描目标自定义模板，达到针对性扫描的目的。
- <导入模板>：导入策略模板，前提是已将相应的策略模板导出到本地。

- <编辑模板>：点击  ，可修改自定义的策略模板。

- <删除模板>：点击  或选中模板，点击  ，可删除用户创建的策略模板。

1. 模板查询

功能描述：用于查询符合条件的模板。

配置路径：【模板】>【策略模板】如下图所示。

图4-6 Web 策略模板-查询

参数说明：

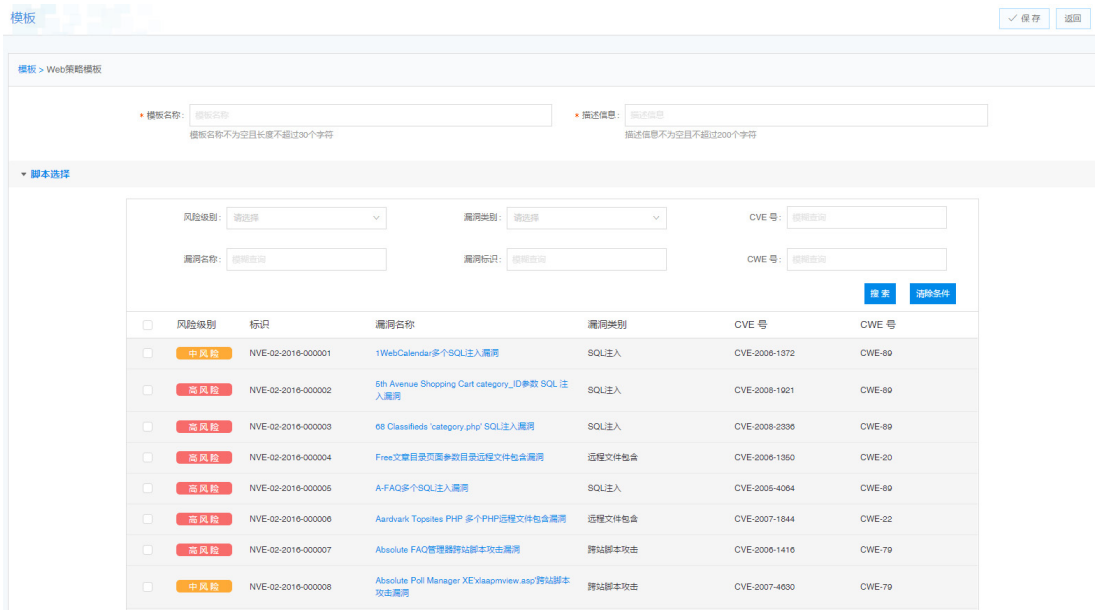
- <策略名称>：在该项中输入相应的名称，即可查询到相应的模板，若是无查询的模板数据，则会提示暂无数据。
- <所属类别>：所属类别有 2 种，分别是“系统”和“用户”。系统自带的模板即为系统模板，系统模板无法进行修改与删除操作，仅能进行查看。用户建立的模板类别为“用户”，是可以进行编辑修改操作。

2. 新建模板

功能描述：根据扫描环境建立新模板，进行有针对性扫描。

配置路径：【模板】>【策略模板】>【Web 策略模板】>【新建模板】如下图所示。

图4-7 Web 策略模板配置



参数说明：

- <策略名称>：输入模板名称。
- <描述信息>：为新建的模板设定描述信息。
- <搜索>：支持按风险级别、漏洞类别、漏洞名称、漏洞标识、CVE 号、CWE 号查询脚本。
- <脚本选择>：默认展示系统内置的 Web 扫描策略，按风险级别和漏洞类型进行分类,通过勾选/取消勾选脚本进行策略模板的配置
- <保存>：配置完成点击<保存>完成 web 策略模板的新建，
- <返回>：点击<返回>则取消新建或修改模板操作。

3. 导入模板

功能描述：导入 Web 策略模板。

配置路径：【模板】>【策略模板】>【Web 策略模板】>【导入模板】如下图所示。

图4-8 Web 策略模板-导入策略模板

导入策略模板的前提要将相应的策略模板导出。点击<选择文件>打开文件选择框，先为导入的模板进行命名。选择要导入的策略模板文件或拖动要导入的文件至导入区域。点击<确定>，将已选择的文件中的策略模板导入漏洞扫描系统。

提示

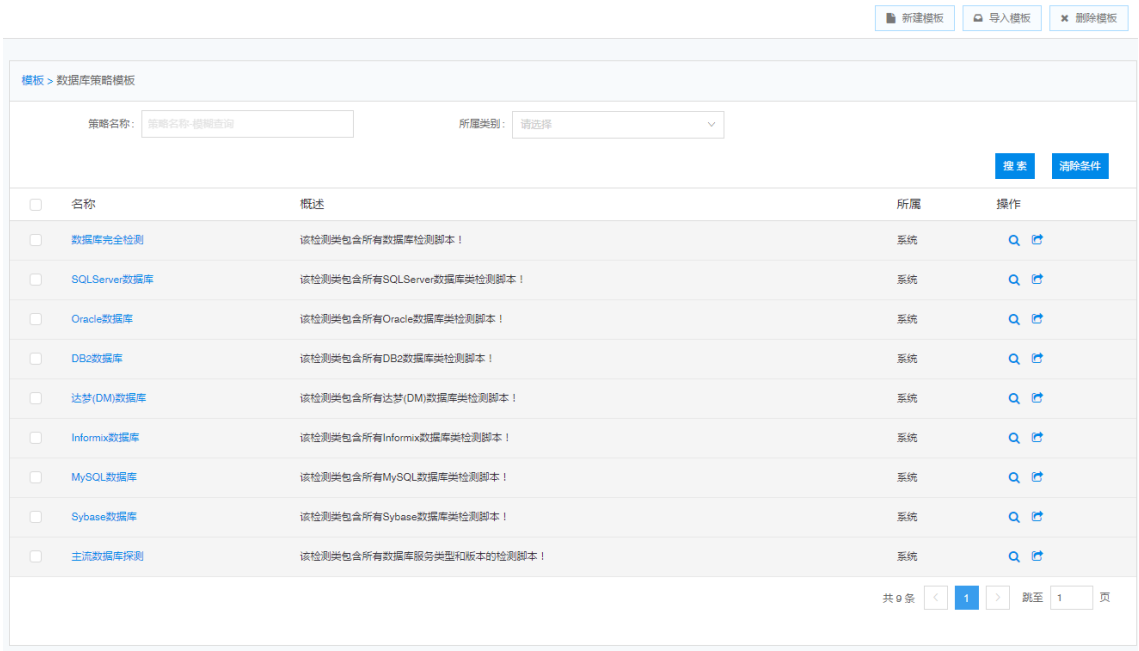
- 导入策略模板的前提是已将相应的策略模板导出并下载到本地磁盘。
- 若模板名与已有的模板重名，或未填写模板名称名，会出现修改或者填写模板名的提示。

4.1.3 数据库扫描策略模板

功能描述：用于配置数据库扫描策略模板，用户可以在该模块下自定义扫描策略。

配置路径：【模板】>【策略模板】>【数据库策略模板】，界面如下图。

图4-9 数据库扫描策略模板



参数说明：

- <搜索>：可对策略模板进行搜索，支持按策略名称、所属类别进行搜索。
- <清除条件>：将输入的搜索条件清空。
- <查看>：点击，可查看模板详情。
- <导出>：点击，可将策略模板下载到本地作为备份，下载的文件格式为 xml。
- <新建模板>：点击 新建模板，跳转到新建策略模板的界面，用户可根据扫描目标自定义模板，达到针对性扫描的目的。
- <导入模板>：导入策略模板，前提是已将相应的策略模板导出到本地。
- <编辑模板>：点击，可修改自定义的策略模板。
- <删除模板>：点击或选中模板，点击 删除模板，可删除用户创建的策略模板。

提示

系统默认的数据库策略模板不能进行修改、删除操作。

1. 模板查询

功能描述：用于查询符合条件的模板。

配置路径：【模板】>【策略模板】如下图所示。

图4-10 数据库扫描策略模板-查询

参数说明：

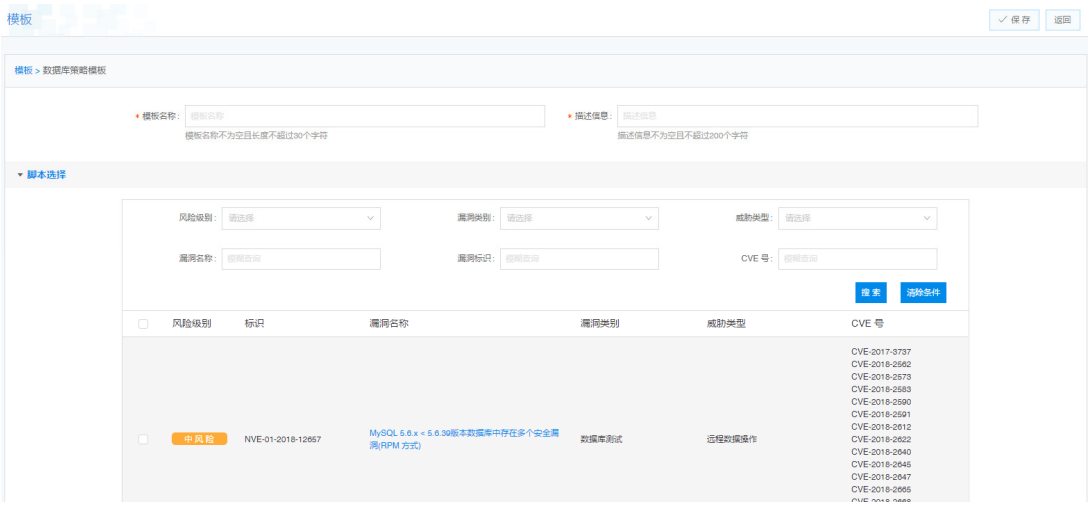
- <策略名称>：在该项中输入相应的名称，即可查询到相应的模板，若是无查询的模板数据，则会提示暂无数据。
- <所属类别>：所属类别有 2 种，分别是“系统”和“用户”。系统自带的模板即为系统模板，系统模板无法进行修改与删除操作。用户建立的模板类别为“用户”，可以进行修改删除操作。

2. 新建模板

功能描述：用户可根据扫描目标自定义主机扫描策略模板，达到针对性扫描的目的。

配置路径：【模板】>【策略模板】>【数据库策略模板】>【新建模板】

图4-11 数据库策略模板-新建



参数说明：

- <模板名称>：输入模板名称。
- <描述信息>：为新建的模板设定描述信息。
- <搜索>：支持按风险级别、漏洞类别、威胁类型、漏洞名称、漏洞标识、CVE 号查询脚本。
- <脚本选择>：默认展示系统内置的主机扫描策略，通过勾选/取消勾选脚本来配置模板，
- <保存>：配置完成点击<保存>完成数据库扫描策略模板的新建，
- <返回>：点击<返回>则取消新建或修改模板操作。

3. 导入模板

功能描述：导入主机扫描策略模板。

配置路径：【模板】>【策略模板】>【数据库策略模板】>【导入模板】如下图所示。

图4-12 数据库策略模板-导入策略模板

导入策略模板的前提要将相应的策略模板导出。先输入模板名称，点击<选择文件>打开文件选择框，先为导入的模板进行命名。选择要导入的策略模板文件或拖动要导入的文件至导入区域。点击<确定>，将已选择的文件中的策略模板导入漏洞扫描系统。

提示

- 导入策略模板的前提是已将相应的策略模板导出并下载到本地磁盘。
- 若模板名与已有的模板重名，或未填写模板名称名，会出现修改或者填写模板名的提示。

4.2 参数模板

功能描述：用于配置主机扫描、数据库扫描、Web 的扫描参数，用户可以根据需要自定义扫描参数。

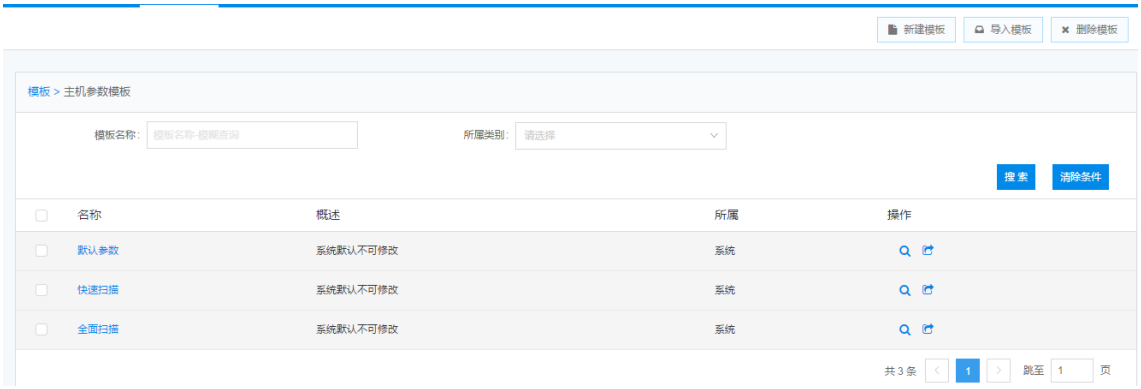
配置路径：【模板】>【参数模板】

4.2.1 主机扫描参数模板

功能描述：用于配置主机扫描参数模板

配置路径：【模板】>【参数模板】>【主机扫描参数模板】

图4-13 主机参数模板



参数说明：

- <搜索>：可对参数模板进行搜索，支持按模板名称、所属类别进行搜索。
- <清除条件>：将输入的搜索条件清空。
- <查看>：点击，可查看 Web 策略模板详情。
- <导出>：点击，可将参数模板下载到本地作为备份，下载的文件格式为 xml。
- <新建模板>：点击 新建模板，跳转到新建参数模板的界面，用户可根据扫描目标自定义模板，达到针对性扫描的目的。
- <导入模板>：导入参数模板，前提是已将相应的参数模板导出到本地。
- <编辑模板>：点击，可修改自定义的参数模板。
- <删除模板>：点击或选中模板，点击 删除模板，可删除用户创建的参数模板。

1. 模板查询

功能描述：查询符合条件的参数模板。

配置路径：【模板】>【参数模板】>【主机参数模板】如下图所示。

图4-14 主机参数模板-查询

参数说明：

- <策略名称>：在该项中输入相应的名称，即可查询到相应的模板，若是无查询的模板数据，则会提示暂无数据。

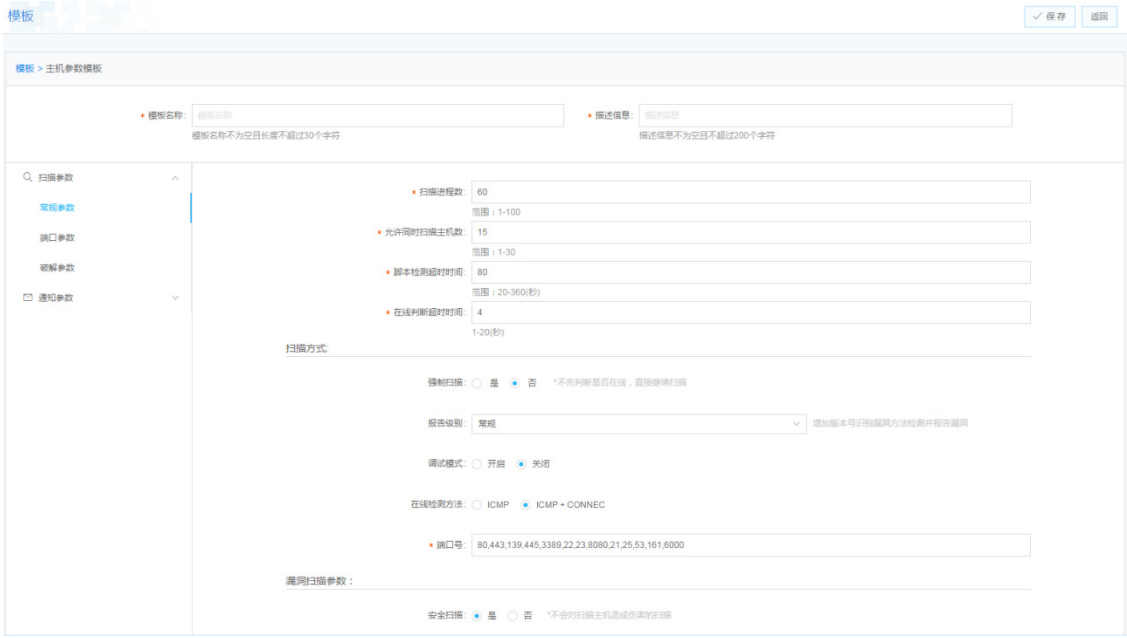
- <所属类别>：所属类别有 2 种，分别是“系统”和“用户”。系统自带的模板即为系统模板，系统模板无法进行修改与删除操作。用户建立的模板类别为“用户”，可以进行修改删除操作。

2. 新建模板

功能描述：根据扫描环境建立新模板，进行有针对性扫描。

配置路径：【模板】>【参数模板】>【主机参数模板】如下图所示。

图4-15 主机参数模板-新建



参数说明：

- <模板名称>：用于输入新建立的模板名称。
- <描述信息>：对模板进行描述。具体参数模板配置可以参照“3.1.2 章节”主机扫描参数，对主机扫描参数进行设置。

3. 导入模板

功能描述：导入主机扫描参数模板。

配置路径：【模板】>【参数模板】>【主机参数模板】>【导入模板】如下图所示。

图4-16 主机参数模板-导入

导入策略模板的前提要将相应的参数模板导出。点击“选择文件”打开文件选择框，先为导入的模板进行命名。选择要导入的策略模板文件或拖动要导入的文件至导入区域。点击“确定”，将已选择的文件中的策略模板导入漏洞扫描系统。

4.2.2 Web参数模板

功能描述：用于配置 Web 参数模板。

配置路径：【模板】>【参数模板】>【Web 参数模板】，界面如下图所示。

图4-17 Web 参数模板

1. 模板查询

功能描述：查询符合条件的参数模板。

配置路径：【模板】>【参数模板】>【Web 参数模板】如下图所示。

图4-18 Web 参数模板-查询

参数说明：

- <策略名称>：在该项中输入相应的名称，即可查询到相应的模板，若是无查询的模板数据，则会提示暂无数据。
- <所属类别>：所属类别有 2 种，分别是<系统>和<用户>。系统自带的模板即为系统模板，系统模板无法进行修改与删除操作。用户建立的模板类别为<用户>，可以进行修改删除操作。

2. 新建模板

功能描述：根据扫描环境建立新模板，进行有针对性扫描。

配置路径：【模板】>【参数模板】>【Web 参数模板】如下图所示。

图4-19 Web 参数模板-新建

参数说明：

- <模板名称>：用于输入新建立的模板名称。
- <描述信息>：对新建立的模板进行描述。具体参数模板配置可以参照“3.1.3”章节 Web 扫描参数，对 Web 扫描参数进行设置。

3. 导入模板

功能描述：导入扫描策略模板。

配置路径：【模板】>【参数模板】>【Web 参数模板】>【导入模板】如下图所示。

图4-20 Web 参数模板-导入

点击<选择文件>打开文件选择框，先为导入的模板进行命名。选择要导入的参数模板文件或拖动要导入的文件至导入区域。点击<确定>，将已选择的文件中的策略模板导入漏洞扫描系统。

提示

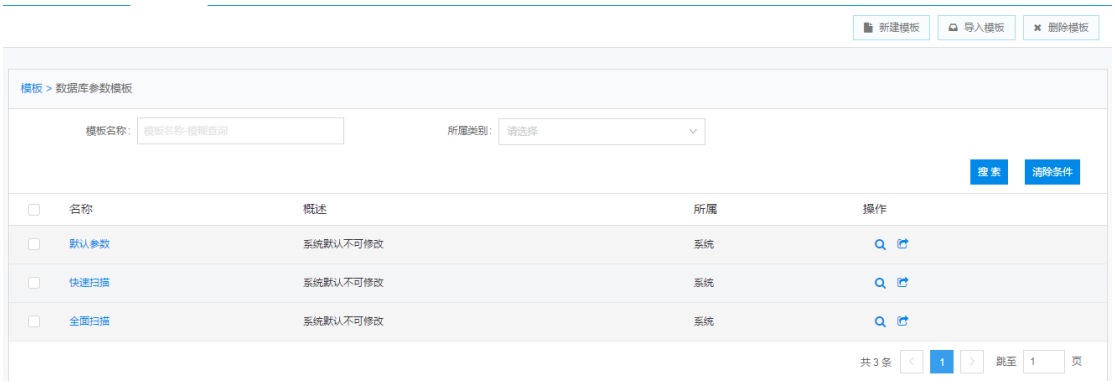
- 导入参数模板的前提是已将相应的参数模板导出并下载到本地磁盘。
- 若模板名与已有的模板重名，或未填写模板名称名，会出现修改或者填写模板名的提示。

4.2.3 数据库扫描参数模板

功能描述：用于配置数据库扫描参数模板

配置路径：【模板】>【参数模板】>【数据库参数模板】

图4-21 数据库参数模板



参数说明：

- <搜索>：可对参数模板进行搜索，支持按模板名称、所属类别进行搜索。
- <清除条件>：将输入的搜索条件清空。
- <查看>：点击，可查看 Web 策略模板详情。
- <导出>：点击，可将参数模板下载到本地作为备份，下载的文件格式为 xml。
- <新建模板>：点击 新建模板，跳转到新建参数模板的界面，用户可根据扫描目标自定义模板，达到针对性扫描的目的。
- <导入模板>：导入参数模板，前提是已将相应的参数模板导出到本地。
- <编辑模板>：点击，可修改自定义的参数模板。
- <删除模板>：点击或选中模板，点击 删除模板，可删除用户创建的参数模板。

1. 模板查询

功能描述：查询符合条件的参数模板。

配置路径：【模板】>【参数模板】>【数据库参数模板】如下图所示。

图4-22 数据库参数模板-查询

参数说明：

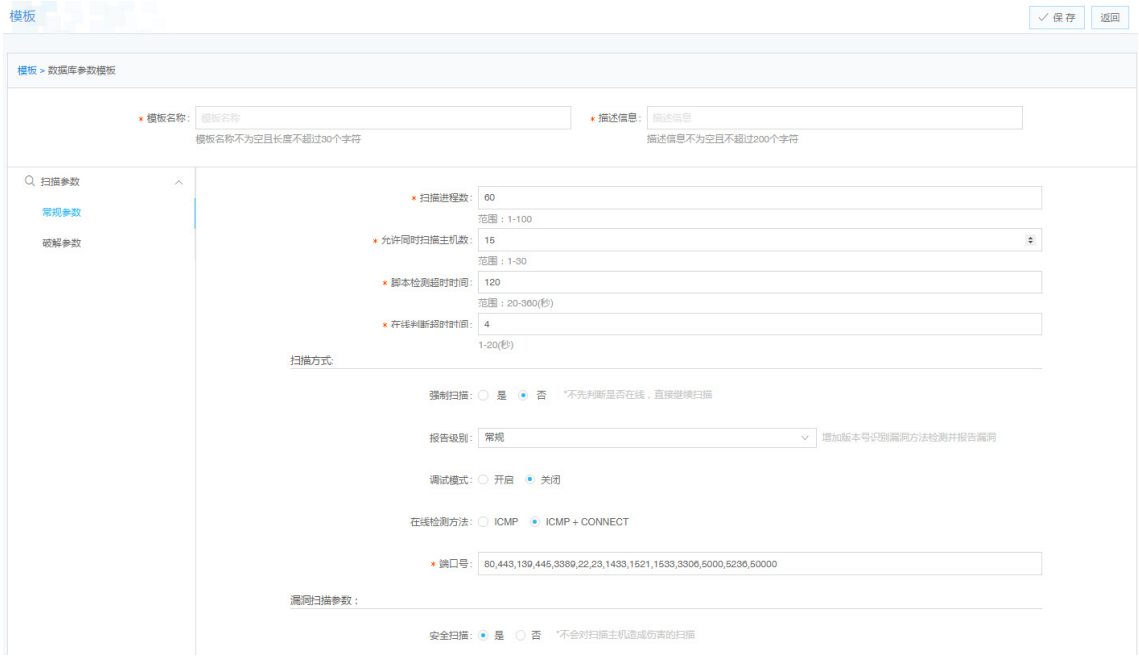
- <策略名称>：在该项中输入相应的名称，即可查询到相应的模板，若是无查询的模板数据，则会提示暂无数据。
- <所属类别>：所属类别有 2 种，分别是<系统>和<用户>。系统自带的模板即为系统模板，系统模板无法进行修改与删除操作。用户建立的模板类别为<用户>，可以进行修改删除操作。

2. 新建模板

功能描述：根据扫描环境建立新模板，进行有针对性扫描。

配置路径：【模板】>【参数模板】>【数据库参数模板】如下图所示。

图4-23 数据库参数模板-新建



参数说明：

- <模板名称>：用于输入新建立的模板名称。
- <描述信息>：对模板进行描述。具体参数模板配置可以参照“3.1.4 章节”数据库扫描参数，数据库扫描参数进行设置。

3. 导入模板

功能描述：导入数据库扫描参数模板。

配置路径：【模板】>【参数模板】>【数据库参数模板】>【导入模板】如下图所示。

图4-24 数据库参数模板-导入

导入策略模板的前提要将相应的参数模板导出。点击“选择文件”打开文件选择框，先为导入的模板进行命名。选择要导入的策略模板文件或拖动要导入的文件至导入区域。点击“确定”，将已选择的文件中的策略模板导入漏洞扫描系统。

4.3 报表模板

功能描述：新建、删除、修改等报表模板管理。

配置路径：【模板】>【报表模板】如下图所示。

图4-25 报表模板

参数说明：

- <搜索>：可对报表模板进行搜索，支持按模板名称、所属类别进行搜索。
- <清除条件>：将输入的搜索条件清空。
- <查看>：点击，可查看报表模板详情。
- <新建模板>：点击 新建模板，跳转到新建模板的界面，用户可根据扫描目标自定义模板，达到针对性扫描的目的。
- <编辑模板>：点击，可修改用户创建的报表模板。
- <删除模板>：点击或选中模板，点击 删除模板，可删除用户创建的报表模板。

4.3.1 报表查询

功能描述：快速查找符合条件的报表。

配置路径：【模板】>【报表模板】如下图所示。

图4-26 报表模板-查询

参数说明：

- <模板名称>：在该项中输入相应的名称，即可查询到相应的模板，若是无查询的模板数据，则会提示暂无数据。
- <所属类别>：所属类别有 2 种，分别是<系统>和<用户>。系统自带的模板即为系统模板，系统模板无法进行修改与删除操作，仅能进行查看。用户建立的模板类别为<用户>，是可以进行编辑修改操作。

4.3.2 新建报表模板

功能描述：创建新的报表模板。

配置路径：【模板】>【报表模板】>【新建模板】如下图所示。

图4-27 报表模板-新建

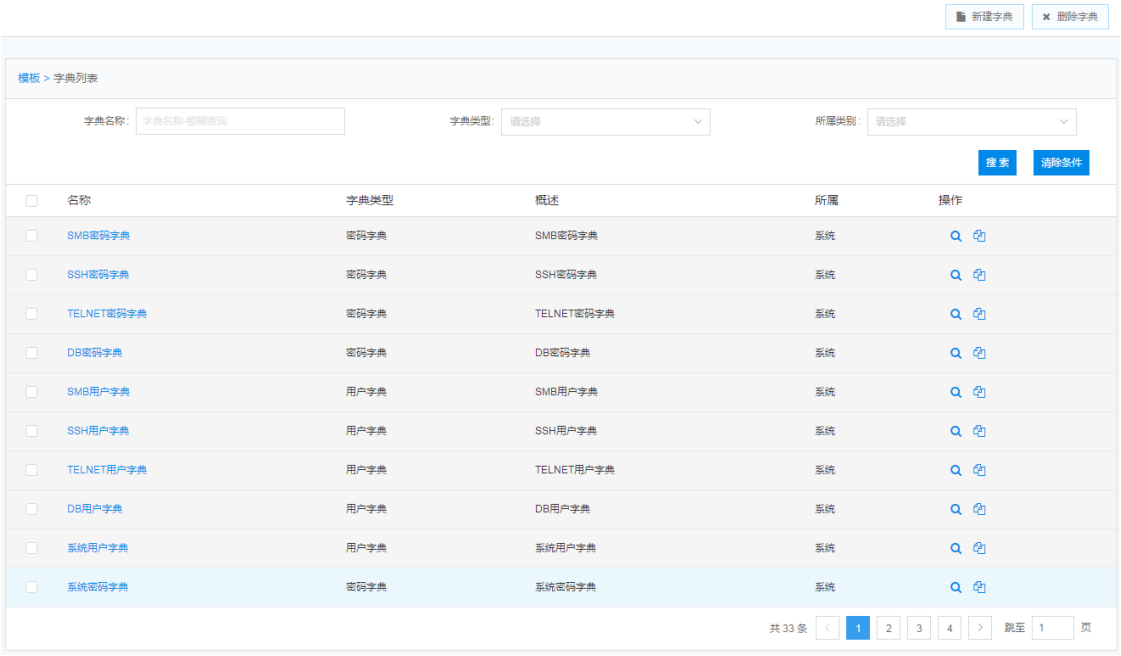
在<新建模板>页面中可以对报表样式、报表封面、报表内容以及风险级别进行定义。可以自定义设置漏洞类别概要信息、安全等级最危险的 IP 数、出现次数最多的漏洞数、显示漏洞的风险级别、操作系统分类统计、服务分类统计、应用分类统计、威胁程度分类统计；可以自定义设置漏洞概要信息排序设置，用户可以按漏洞编号、风险级别、漏洞类别、漏洞详细信息、漏洞编号、风险级别等。点击<保存>保存当前报表样式的所有内容。

4.4 数据字典

功能描述：配置用户名和密码字典，用于账号密码破解。

配置路径：【模板】>【数据字典】如下图所示。

图4-28 数据字典



参数说明：

- <搜索>：可对字典进行搜索，支持按字典名称、所属类别进行搜索。
- <清除条件>：将输入的搜索条件清空。
- <查看>：点击，可查看字典详情。
- <复制>：点击，可复制字典。
- <编辑>:点击，可修改字典相关信息。
- <新建字典>：点击，跳转到新建模板的界面，用户可根据扫描目标自定义模板，达到针对性扫描的目的。
- <删除字典>：点击或选中模板，点击，可删除用户创建的字典。

4.4.1 字典查询

功能描述：快速查找符合条件的字典。

配置路径：【模板】>【数据字典】如下图所示。

图4-29 数据字典-查询

参数说明：

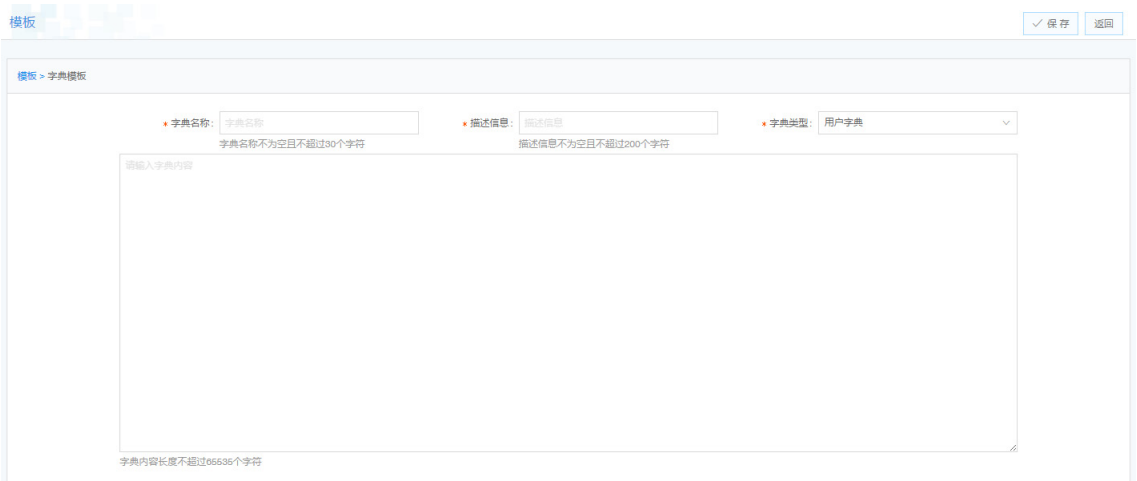
- <字典名称>：中输入相应的名称，即可查询到相应的字典，若是无查询的字典数据，则会提示暂无数据。
- <字典类型>：字典类型有 2 种，分别是用户登录名称字典以及登录密码字典。
- <所属类别>：支持全部，系统和用户查询

4.4.2 新建字典

功能描述：新建设用户名或密码字典，用于账号密码破解。

配置路径：【模板】>【数据字典】>【新建字典】如下图所示。

图4-30 数据字典-新建



用户字典和密码字典内容格式为一行一个字典数据项，点击<保存>按钮，可保存新建内容，并返回到密码破解页面。

5 系统管理与配置

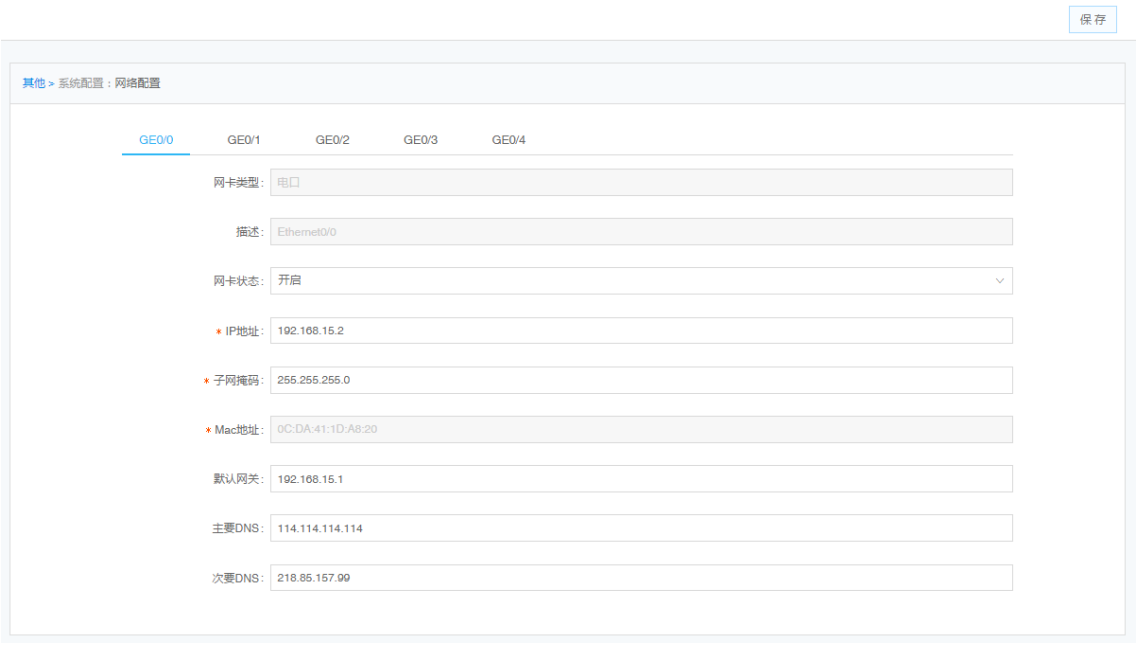
系统管理与配置主要为用户提供对系统配置和帐户信息的管理和操作的接口。在系统管理模块中，用户可以进行资产管理、网络设置、时间设置、SMTP 设置、日志管理、帐户管理、角色管理、密码修改、数据备份、重新启动以及关机等操作。网络设置提供系统网络设置的接口，包括系统 IP、子网掩码、网关、DNS 和路由设置。时间设置可查看、修改系统时间，可获取客户端系统时间。SMTP 设置用来设定系统发送邮箱所使用的邮件服务器。日志管理可以查询一定时期内系统发生的各种事件日志，例如用户登录、帐户管理、策略管理等。帐户管理可以增加、修改、删除帐户。角色管理可以增加、修改、删除角色，方便用户权限的分配。数据备份提供备份数据库和恢复数据库，用户备份数据库后，需要恢复数据库时可通过恢复数据库来恢复数据库数据。

5.1 网络设置

功能描述：接口 IP、子网掩码、网关、DNS 等基本网络设置配置。

配置路径：【其它】>【系统配置】>【网络配置】，如下图所示。

图5-1 网络配置



选择系统管理菜单下的【其它】>【系统配置】>【网络配置】，进入网络设置页面。用户选择所要配置的网卡，输入相关信息包括 IP 地址、子网掩码；输入系统默认网关；输入 DNS 域名服务器的 IP 地址，最多可设两个。输入正确并提交设定后则系统的网络配置将改变。如果系统的 IP 改变，则必须使用新的 IP 重新登录。不同网卡不能设置相同的网段，否则会造成网络不通。如果当前设置的网卡对应的网口未接上网线，并且设置的网段和当前用户所在的网段一样，那么将会造成当前用户无法继续连接系统。如果设置网卡时修改了浏览器上显示的 IP 地址，点击<保存>生效后，当前连接会被断开，请使用新的 IP 地址重新连接。默认网关必须设置为某个有效网卡所在网段的网关，这样才能转发数据。如果用户删除了默认网关对应的网卡，则默认网关也将失效，将会造成部分主机无法继续连接。

DNS 指系统连接域名时所使用的域名解析服务器，负责把域名转换成为网络可以识别的 IP 地址。如果 DNS 未设置正确，可能造成无法扫描域名，或者使用域名地址（如默认的升级地址）在线升级时无法连接升级服务器。

5.2 路由设置

功能描述：添加、删除路由。

配置路径：【其它】>【系统配置】>【路由设置】如下图所示。

图5-2 路由设置

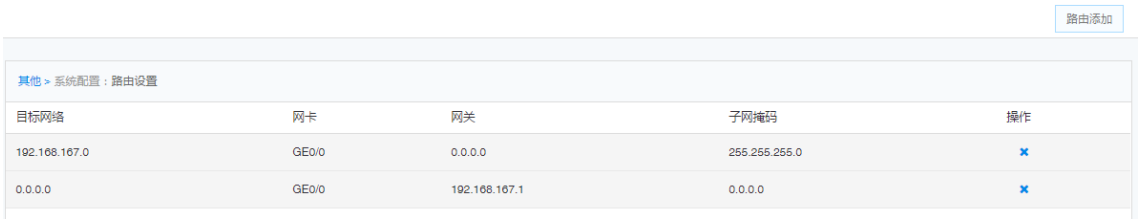


图5-3 路由添加

点击<路由设置>进入路由设置页面，可以根据需要添加、删除路由。注意：路由设置不当将导致系统无法被访问，设置时请认真核对。路由表存储了本地计算机可以到达的网络目的地址范围和如何到达的路由信息。目标主机或网络与子网掩码用于定义本地计算机可以到达的网络目的地址范围。网关是指在发送 IP 数据包时，针对特定的网络目的地址，数据包发送到的下一个目标地址。网关设置为 0.0.0.0 表示没有网关，数据包直接发送到目的地址。网卡号定义了针对特定的网络目的地址，本地计算机用于发送数据包的网卡。网卡号的 GE0/0、GE0/1、GE0/2、GE0/3、GE0/4、GE0/5 分别对应了 6 张网卡，lo 指本机。设置路由表时，如果网卡号对应的网卡未设置 IP 地址，则不能添加该网卡号的路由。网关如果不是 0.0.0.0，则必须设置为和网卡号对应的 IP 地址相同的网段内，否则会造成在使用此路由项时需调用其他路由项，从而可能会导致路由死锁。目标主机或网络为 0.0.0.0，网关为默认网关，网络掩码为 0.0.0.0 的路由称为默认路由。当到达特定主机或特定子网的路由并未在路由表中指定时，均通过默认路由来进行转发。如果没有设置默认路由，那么无法到达未在路由表中指定路由项的网络目的地址。

5.3 时间配置

功能描述：设置系统时间。

配置路径：【其它】>【系统配置】>【时间设置】如下图所示。

图5-4 时间设置

5.4 通讯配置

功能描述：设置扫描器与产品提供内置端浏览器通信，需要使用当前访问的扫描器 IP 地址，实现手动爬行和被动扫描。

配置路径：【其它】>【系统配置】>【通讯配置】，如下图所示。

图5-5 通讯设置

5.5 磁盘设置

功能描述：磁盘空间达到设置的磁盘空间上限，系统将发出告警，并且影响任务创建，需要清理历史任务。

配置路径：【其它】>【系统配置】>【磁盘设置】如下图所示。

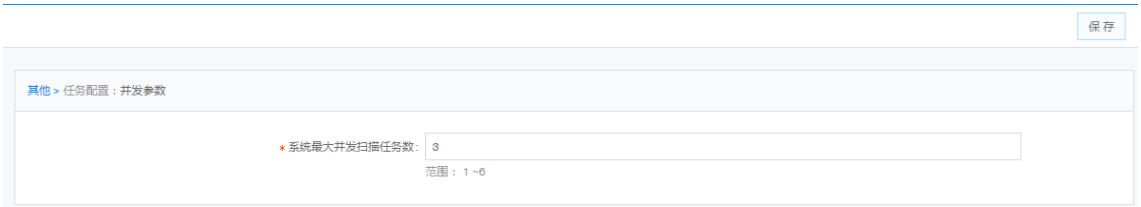
图5-6 磁盘设置

5.6 并发参数

功能描述：最大并发扫描任务数和最大并发扫描主机数。

配置路径：【其它】>【任务配置】>【并发参数】如下图所示。

图5-7 并发参数设置



“系统最大并发扫描任务数”是指系统最多可同时运行的扫描任务数。允许同时扫描任务数越多，系统的扫描效率越高，但任务数到达一定数目后，将增加系统的负荷，系统效率提高有限。此参数的允许范围和默认优化值因产品型号不同而不同。

5.7 评估参数

功能描述：设定生成报表中的漏洞风险等级、网络安全等级标准分值等网络安全评估参数。

配置路径：【其它】>【任务配置】>【评估参数】，如下图所示。

图5-8 评估参数设置

参数说明：

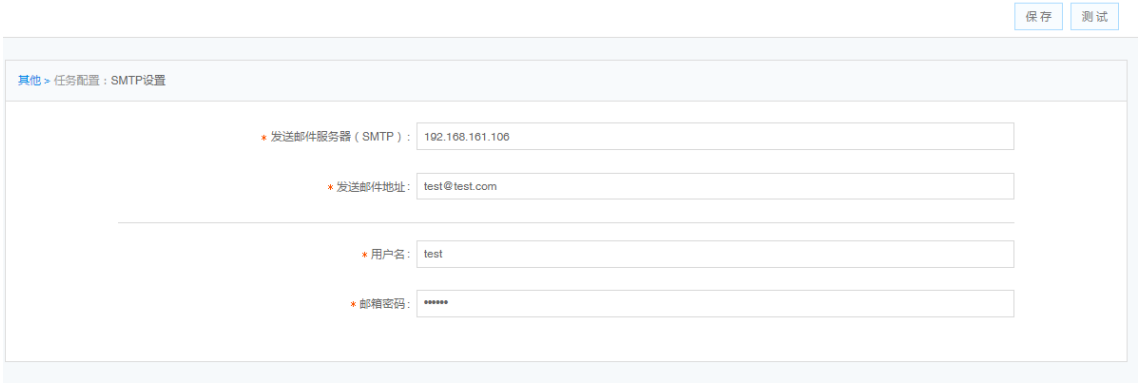
- <漏洞风险等级对应分值>：漏洞风险分为紧急、高风险、中风险、低风险、信息五个等级。
- <紧急>：可能被恶性病毒所利用造成网络大范围瘫痪。
- <高>：攻击者可以远程执行任意命令或者代码；攻击者可以远程获取应用系统的管理权限；远程拒绝攻击服务。
- <中>：攻击者可以远程创建、修改、删除文件；可以任意读取文件目录；可以获得用户名、口令等敏感信息，潜在可能导致高风险的漏洞。
- <低>：攻击者可以获得某些系统、服务的信息，如版本号、操作系统类型等。
- <信息>：主要为配合以上类别的检测。
- <单机评估安全等级分值>：单机安全等级分为四个等级：安全、比较安全、比较危险、危险。单机安全等级以单机扫描出的所有漏洞的分险等级分值之和乘以该主机资产值来评估。

5.8 SMTP设置

功能描述：设置是用于设置发送定时扫描的邮件报告和扫描邮件通知所必须的 SMTP 服务器信息。如果未设置或者设置不正确，系统将无法发送定时扫描的邮件报告和扫描邮件通知。

配置路径：【其它】>【任务配置】>【SMTP 设置】，如下图所示。

图5-9 SMTP 设置



参数说明：

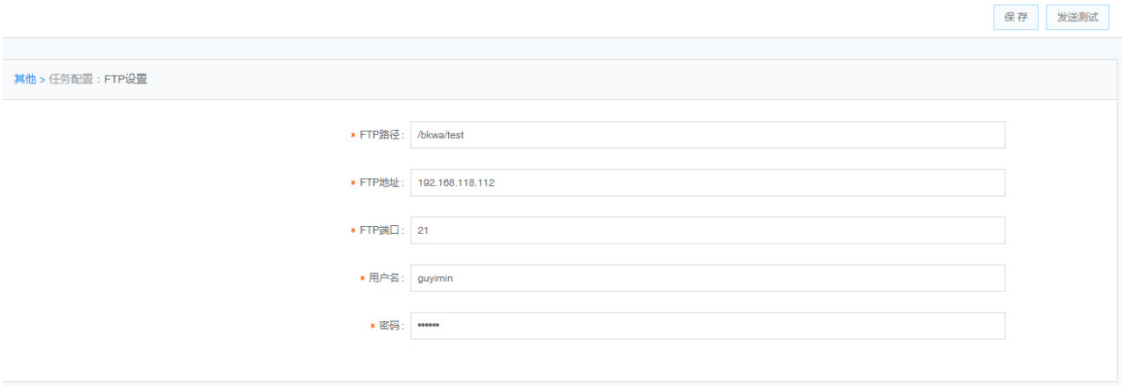
- <发送邮件服务器>：用于设置发送邮件服务器的域名或 IP，例如 sina 邮箱的发送邮件服务器的域名为 smtp.sina.com。
- <发送邮件地址>：发送邮件地址为发件人的邮箱地址，如***@sina.com。
- <邮件服务器身份验证>：若该邮件服务器发送邮件需要身份验证，则用户需填写<用户名>和<邮箱密码>。
- <保存>：配置完毕后，点击<保存>按钮，即可保存 SMTP 设置。
- <发送测试>：系统会采用设置的 SMTP 信息，发送测试邮件到“发送邮件的 SMTP 地址”中，用户可到该邮箱地址中接收测试邮件。如果收到，则说明设置正确。如果没有收到测试邮件，说明设置有错误，请修改设置。

5.9 FTP设置

功能描述：用于设置 FTP 服务器信息，设置正确的情况下，若扫描任务开启了<上传结果到 FTP>，则扫描结束后系统会将扫描报表上传到设定的 FTP 目录。

配置路径：【其它】>【任务配置】>【FTP 设置】，如下图所示。

图5-10 FTP 设置



参数说明：

- <FTP 路径>：用于设置上传路径，例如/home/bkwa。
- <FTP 地址>：用于设置 FTP 服务器的 IP 地址。
- <FTP 端口>：配置 FTP 端口，例如 21。
- <用户>：用于配置 FTP 用户，该用户必须有权限访问 FTP 路径。
- <密码>：用于配置 FTP 用户的密码。
- <保存>：保存 FTP 配置。
- <发送测试>：系统会采用设置的 FTP 配置，上传测试文件到配置的 FTP 路径，FTP 用户可到 FTP 路径查看是否接收到测试文件。如果 FTP 路径下存在测试文件，说明设置正确。反之，说明设置有错误，请修改设置。

5.10 系统服务配置

功能描述：系统 SSH 服务、SNMP 服务开关。

配置路径：【其它】>【服务配置】，如下图所示。

图5-11 服务配置

SSH 服务开启指允许管理员通过 SSH 连接漏洞扫描系统，关闭则表示禁止通过 SSH 连接漏洞扫描系统；SNMP 服务开启表示通过通过 SNMP 访问漏洞扫描系统，在“团体名称”输入框内输入团体名称；关闭则表示禁止通过 SNMP 访问漏洞扫描系统。点击“保存”保存服务配置参数。

5.11 关于

功能描述：展示产品信息、公司信息，以及服务器资源占用情况等。

配置路径：【其它】>【关于】

5.11.1 产品信息

功能描述：展示产品相关信息，包括产品基本信息、产品使用授权信息、功能模块信息、设备 hash 值以及更换授权文件等功能。

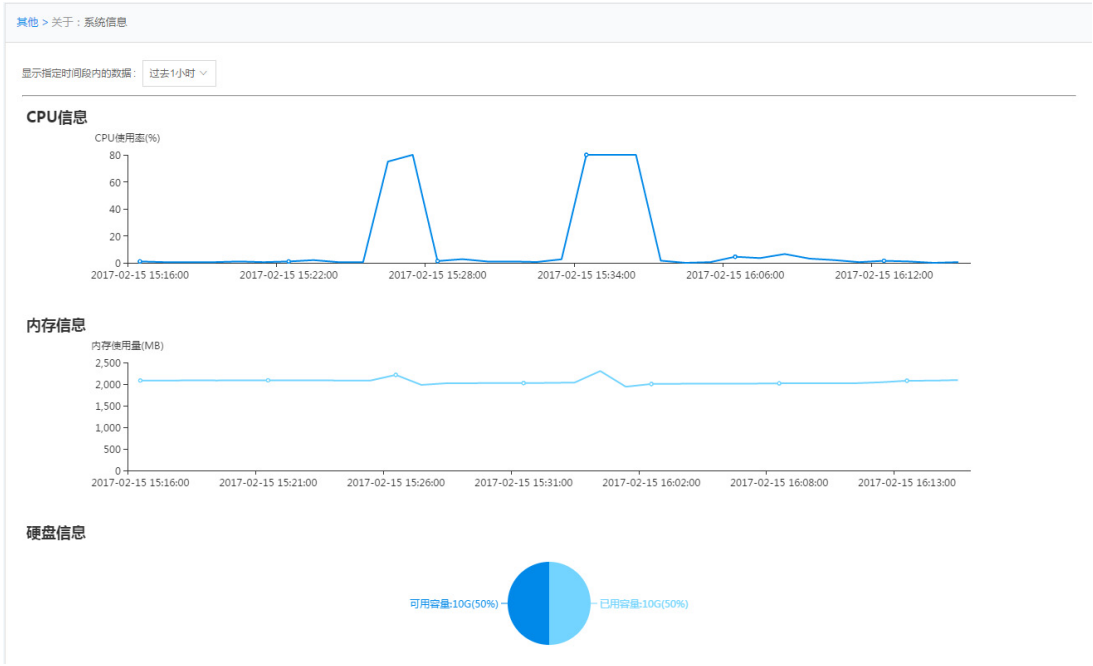
配置路径：【其它】>【关于】>【产品信息】。

5.11.2 系统信息

功能描述：展示目前服务器资源占用情况。

配置路径：【其它】>【关于】>【系统信息】，如下图所示。

图5-12 系统信息



5.11.3 公司网站

功能描述：跳转至公司门户网站，为客户展示更多公司产品。

配置路径：【其它】>【关于】>【公司网站】

5.12 系统升级

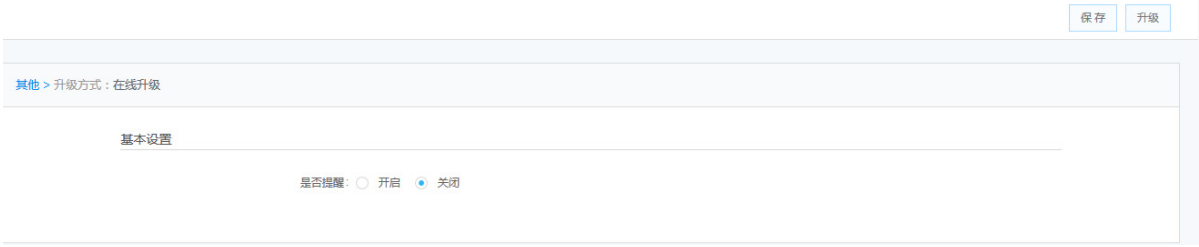
升级模块包括在线升级、离线升级、定时升级。

5.12.1 在线升级

功能描述：在线方式升级漏洞扫描系统的程序和漏洞库。

配置路径：【其它】>【升级方式】>【在线升级】，如下图所示。

图5-13 在线升级配置



点击<保存>保存配置。点击<升级>进入选择升级包页面，如下图所示。

图5-14 在线升级页面

5.12.2 离线升级

功能描述：离线方式（本地）升级漏洞扫描系统的程序和漏洞库。

配置路径：【其它】>【升级方式】>【离线升级】如下图所示。

图5-15 离线升级

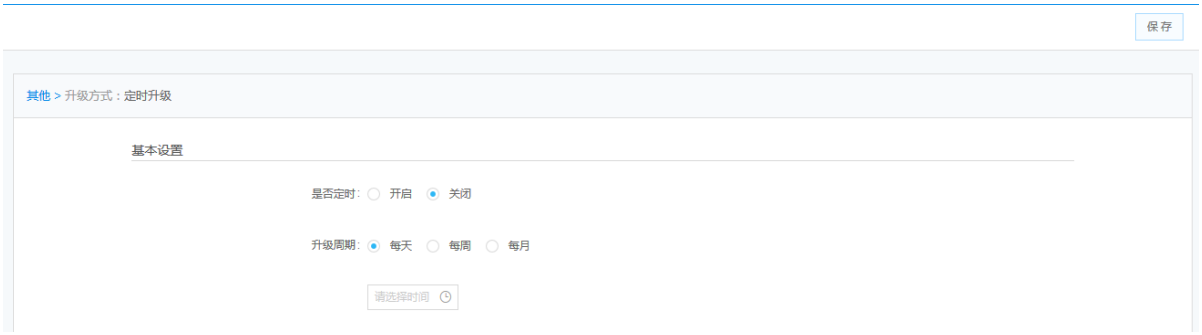
如果系统不能上网或者网络速度较慢，可以选择离线升级。先把升级包下载到本地主机，然后通过本地主机访问系统，进入离线升级，点击“选择文件”选择存在本地主机上的升级包后，开始升级。

5.12.3 定时升级

功能描述：定时自动在线升级漏洞扫描系统的程序和漏洞库。

配置路径：【其它】>【升级方式】>【定时升级】如下图所示。

图5-16 定时升级



定时升级可以设定系统在指定的时间自动在线升级，升级周期包括“每天”、“每周”和“每月”三种：

- <每天>指系统每天在指定的时间自动在线升级。
- <每周>指在每周的指定星期的定时时间自动在线升级。
- <每月>指系统将在每月的指定日期的定时时间自动在线升级。

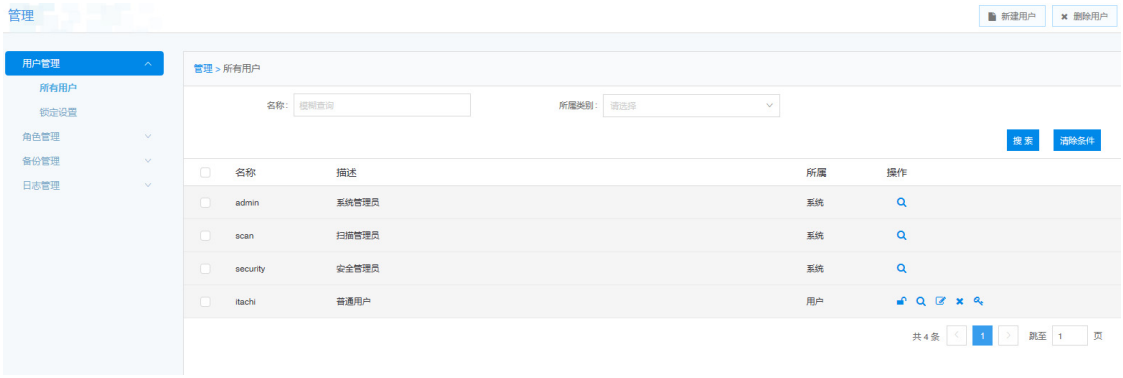
点击“保存”保存配置。

5.13 用户管理

功能描述：用户及用户权限管理。

配置路径：【管理】>【用户管理】如下图所示。

图5-17 用户管理



<用户管理>页面默认将列出系统所有的帐户（除了审计管理员 audit）。系统内置账户包括 admin\audit\scan\security 四个账户，对应的角色分别为系统管理员、审计管理员、扫描管理员、安全管理员。不同角色的用户相互制约，系统管理员拥有系统配置及管理权限，但没有用户管理、日志审计等权限；审计管理员权限范围为日志审计，安全管理员的权限范围包括用户管理、角色管理、备份管理以及对审计管理员的操作。

如果管理员要修改或删除某个帐户，点击其后的 或 ，即可修改或删除相应的帐户。用户还可以设置登录锁定，对登录错误的帐户进行加锁和解锁。点击 可锁定帐户，该账户将无法登录系统。如果登录锁定中设置的锁定时间大于 0，被管理员加锁的帐户在锁定时间之后会自动解锁。点击 ，可解除对该帐户的锁定。点击 可以对非系统账户进行密码重置操作。

5.13.1 用户查询

功能描述：查询符合条件的用户。

配置路径：【管理】>【用户管理】如下图所示。

图5-18 用户查询

参数说明：

- <账号>：用户账号。
- <名称>：用户名。
- <用户状态>：用户账号状态分为正常和锁定。
- <搜索>：可对用户进行搜索，支持按账号、名称、用户状态组合条件搜索。
- <清除条件>：将输入的搜索条件清空。

5.13.2 锁定设置

功能描述：允许账户最大错误登录次数、账户锁定时间、会话时间等功能设置。

配置路径：【管理】>【用户管理】>【锁定设置】如下图所示。

图5-19 锁定设置

参数说明：

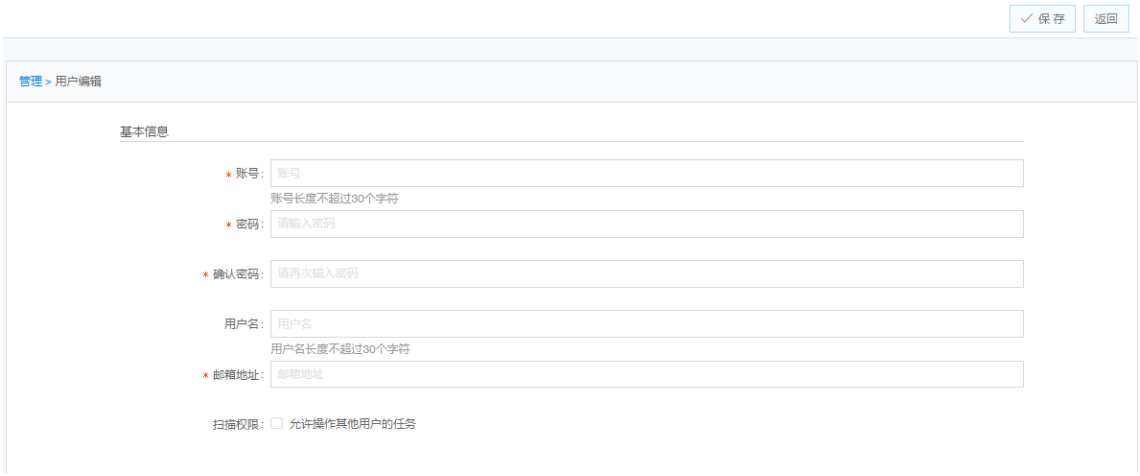
- <允许最大错误登录次数>：指允许用户以及 IP 地址连续错误登录的次数，如果用户以及 IP 地址登录失败的次数大于等于设定的最大错误登录数时，该用户帐号以及 IP 地址会被锁定。
- <错误登录锁定时间>：同一 IP 主机登录失败大于等于最大错误次数时 IP 地址会被锁定，直到系统设置的解锁时间之后或 12 小时后自动解锁。该值如果设为 0，表示需要管理员解锁。
- <会话超时时间>：会话空闲时间，即在超时时间内未进行任何操作，则系统将自动退出登录，系统缺省配置为 3 分钟。
- <密码更换周期>：指密码有效时间，到达密码更换周期后必须更改密码。
- <密码最短长度>：配置密码最短的长度。
- <密码复杂度>：密码组成的配置项。
- <保存>：保存并生效锁定设置。

5.13.3 新建用户

功能描述：允许账户最大错误登录次数、账户锁定时间、会话时间等功能设置。

配置路径：【管理】>【新建用户】如下图所示。

图5-20 用户基本信息编辑



在<基本信息>标签中，填写用户名、密码、确认密码、用户说明和邮箱地址，邮箱地址用来接收定时扫描邮件报告、扫描完毕通知邮件等,勾选扫描权限，允许操作其他用户的任务的权限。

图5-21 设置 IP 地址限制

参数说明：

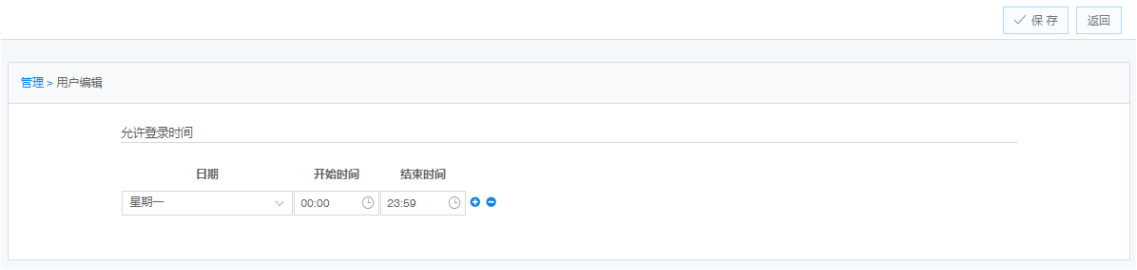
- <可扫描 IP 地址>：指设定对新建的用户可扫描 IP 地址和允许登录 IP 地址做设定。如果该栏目没有进行任何设置，则表示不限制该帐户的可扫描 IP 范围，该帐户的可扫描 IP 范围将与系统可扫描 IP 范围一致。如果设定新建帐户只能对单个 IP 或者单个域名主机扫描，则直接输入单个 IP 或者单个域名；如果设定新建的用户能对多 IP 扫描，则输入 IP 范围或者 IP 子网，如 192.168.168.1-192.168.168.5，多个范围通过逗号（,）隔开。
- <允许登录 IP 地址>：指用户可设定新建帐户可从哪个 IP 登录。如果该栏目没有任何设定，则表示不限制该帐户的登录 IP 地址。如果设定新建的帐户只能从单个 IP 登录，则输入单个 IP，如果设定新建的用户能从多 IP 登录，则输入 IP 范围或者 IP 子网。如下图所示。

图5-22 设置可扫描 URL 地址

参数说明：

- <URL 地址限制>：指设定对新建的用户可扫描 URL 地址做设定。如果该栏目没有进行任何设置，则表示不限制该帐户的可扫描 URL 地址范围。合法的 URL 地址必须以 http://或 https://开头，*匹配任意多个字符，?匹配单个字符。

图5-23 设置允许登录时间



参数说明：

- <登录时间限制>：指设定新建帐户可以在哪些时间段登录系统。如果该栏目没有任何设定，则表示不限制该帐户的登录时间。选择具体时间，则表示只允许选择的时间段内允许登录系统，如下图所示。
- <保存>：保存并创建新建用户。

5.14 角色管理

功能描述：角色管理，系统内置 4 个角色，分别是 admin（系统管理员）、audit（审计管理员）、security（安全管理员）、scan（扫描管理员），每个角色的权限不同，以此达到三权分立的目的。

配置路径：【管理】>【角色管理】如下图所示。

图5-24 角色管理

参数说明：

- <搜索>：支持按角色名称进行搜索。
- <查看角色详情>：点击 ，可查看角色名称、角色描述、角色权限。
- <编辑>：只有 scan 这个角色支持编辑，点击 ，可修改角色名称、角色描述。
- <配置该角色的用户>：admin、audit、security 三个角色不支持配置其他用户，新建的用户只能配置为 scan 管理员，点击 ，进行用户配置。

具体的用户权限如下表所示。

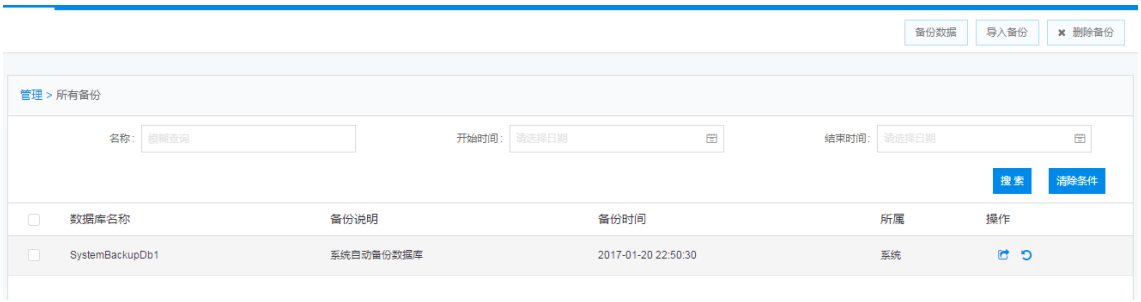
用户角色	系统用户	权限
系统管理员（admin）	admin	扫描、模板、资产管理、工具、系统配置、任务配置、服务配置、升级、关于等权限，无用户管理、日志审计权限，以及查看和修改自身用户信息，修改自身密码的权限
安全保密管理员（security）	security	用户管理、角色管理、备份管理、以及对审计员的操作进行日志审计的功能权限，以及查看和修改自身用户信息，修改自身密码的权限
审计管理员（audit）	audit	只具有日志审计功能权限，以及查看和修改自身用户信息，修改自身密码的权限
扫描管理员（scan）	scan	扫描、模板、资产管理、工具功能权限，以及查看和修改自身用户信息，修改自身密码的权限

5.15 备份管理

功能描述：备份数据、恢复数据库、导入、删除备份数据等。

配置路径：【管理】>【备份管理】如下图所示。

图5-25 备份管理



参数说明：

- <备份数据>：备份的数据库内容包括历史扫描任务、扫描参数设置、定时扫描任务、评估参数设置、策略、SMTP 设置、日志管理、帐户、角色等系统数据。点击右上角“备份数据”调出如下对话框，输入数据库名称、描述、备份时间点击确定系统将自动进行数据备份。

图5-26 备份数据库

- <恢复数据>：点击备份数据库列表中的某个数据库后，并点击“恢复数据”，系统提示是否恢复数据库，点击“确定”按钮进入恢复数据库页面，恢复当前数据库为备份的数据库；点击“取消”按钮取消操作。恢复数据库过程中，系统将无法正常使用。恢复数据库后请重新启动服务器，否则可能无法正常访问系统！数据库恢复成功后，系统将提示用户重新启动服务器以使新的数据库生效。
- <删除备份>：点击备份管理列表中某个数据库后的“删除备份”按钮，系统提示是否确认删除备份数据库，点击“确定”按钮删除备份数据库，点击“取消”按钮取消操作。数据库删除成功后，系统将提示用户删除成功。
- <导入备份>：点击“导入备份”按钮，进入备份数据库导入对话框，选择本地的备份数据库文件后，点击“确定”按钮，系统会将本地备份数据库导入到系统中，如下图所示。

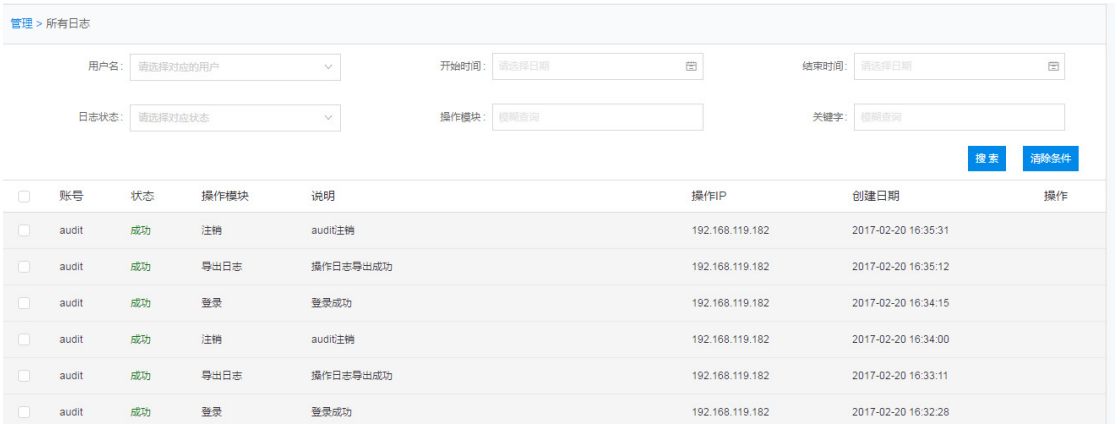
图5-27 导入数据库备份

5.16 日志管理

功能描述：日志查询管理。

配置路径：【管理】>【日志管理】如下图所示。

图5-28 日志管理



security 账号登录点击[【日志管理】只能看到审计管理员 audit 的操作日志。输入开始时间和结束时间，即可查询到相应时间的操作日志；登录 audit 账号，点击【日志管理】进入日志管理的查询窗口。输入开始时间和结束时间，即可查询到相应时间的操作日志。

5.16.1 日志配置

功能描述：日志管理配置。

配置路径：【管理】>【日志配置】如下图所示。

图5-29 日志配置

参数说明：

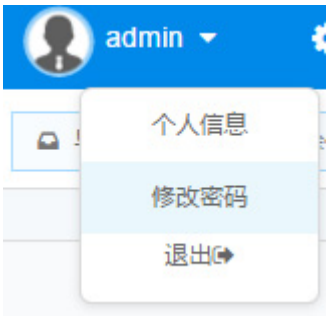
- <日志备份提醒>：根据上次备份日期时间，定时提醒备份日志。“日志删除提醒”当日志记录超过指定条数后，会进行提醒。“日志删除设置”会根据配置的时间，系统会定时进行日志删除操作。配置完成后点击右上角<保存>配置即时生效。
- <Syslog 服务器地址配置>：开启后，会向设定的 IP 地址发送日志记录。

5.17 修改密码

功能描述：修改当前用户密码。

配置路径：【用户头像】>【修改密码】如下图所示。

图5-30 修改密码



点击用户名头像下拉菜单中的<修改密码>，进入修改密码页面，用户可以进行当前用户的密码修改。用户必须输入旧密码和两次新密码。如果旧密码正确，输入的两次新密码一致，则修改密码成功。否则，修改密码失败。

5.18 获取版本信息

功能描述：获取当前版本信息。

配置路径：【？图标】如下图所示。

图5-31 版本信息

点击右上角  图标，查看漏洞扫描系统的版本信息。

5.19 关机重启

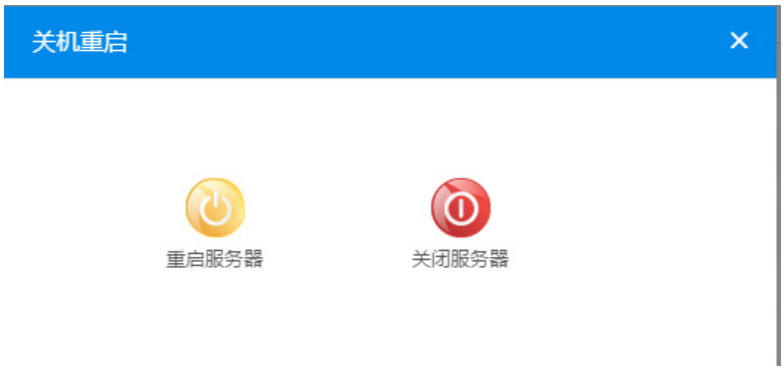
功能描述：重启关闭服务器功能。

配置路径：【电源图标】如下图所示。

图5-32 电源

点击右上角  图标，根据需要选择重启服务器或关闭服务器。

图5-33 关机重启



6 常用工具

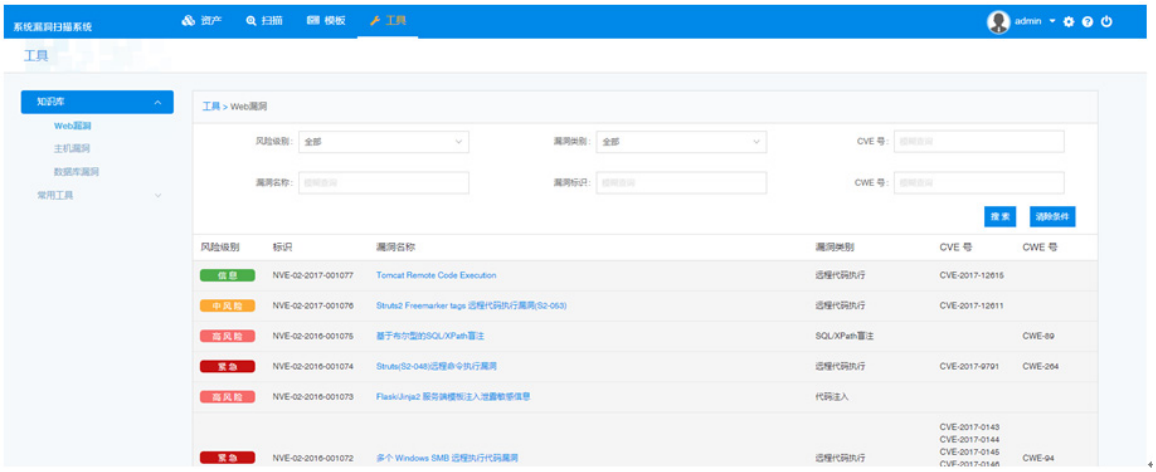
系统内置了丰富的常用工具，包括知识库查询、目标主机检测、端口扫描、密码破解、加解密、HTTP等工具。

6.1 知识库查询

功能描述：漏洞知识库查询管理，包含主机漏洞知识库以及 Web 漏洞知识库。

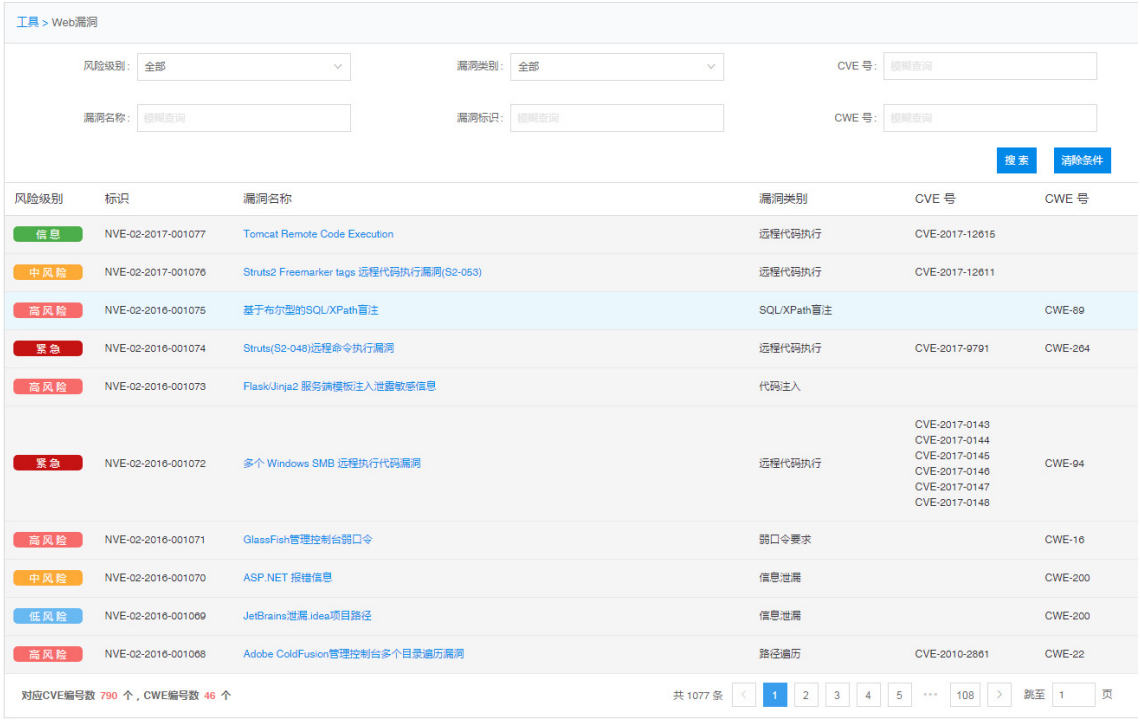
配置路径：【工具】>【知识库】如下图所示。

图6-1 知识库



6.1.1 Web漏洞

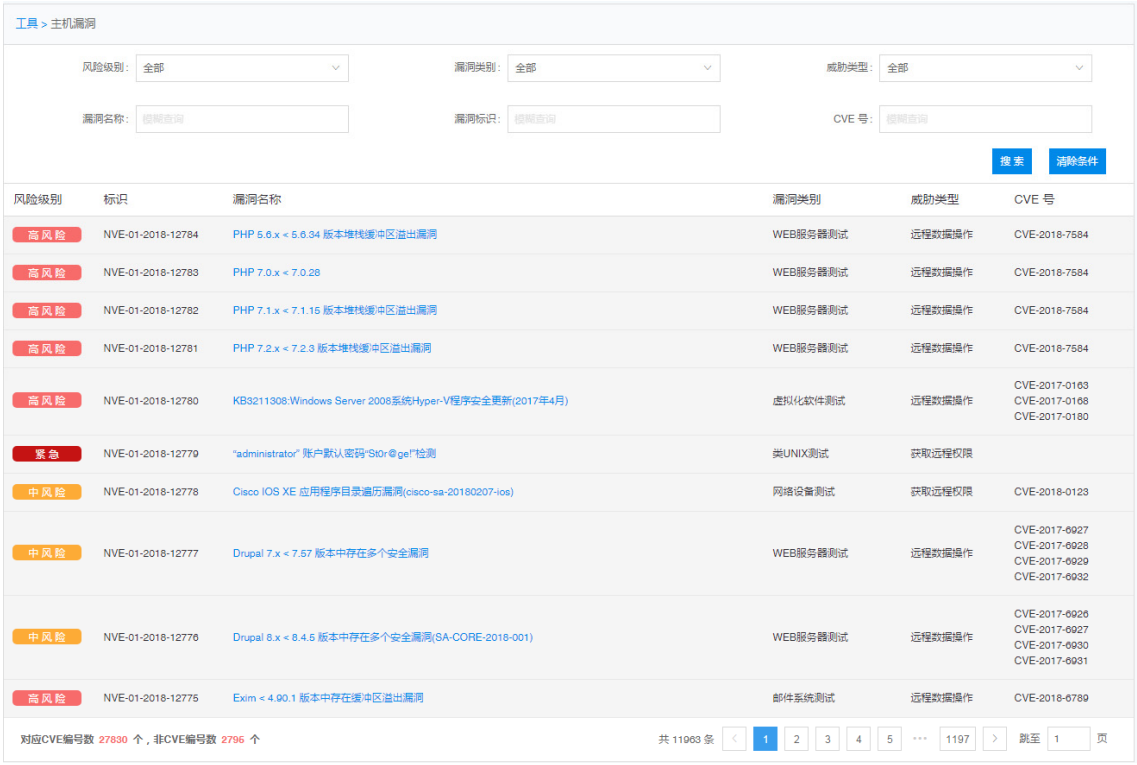
图6-2 知识库-Web 漏洞



Web 漏洞知识库包括风险级别、内部漏洞标识、漏洞名称、漏洞类别、CVE 号等知识，方便管理员对相关漏洞知识快速、全面了解。

6.1.2 主机漏洞

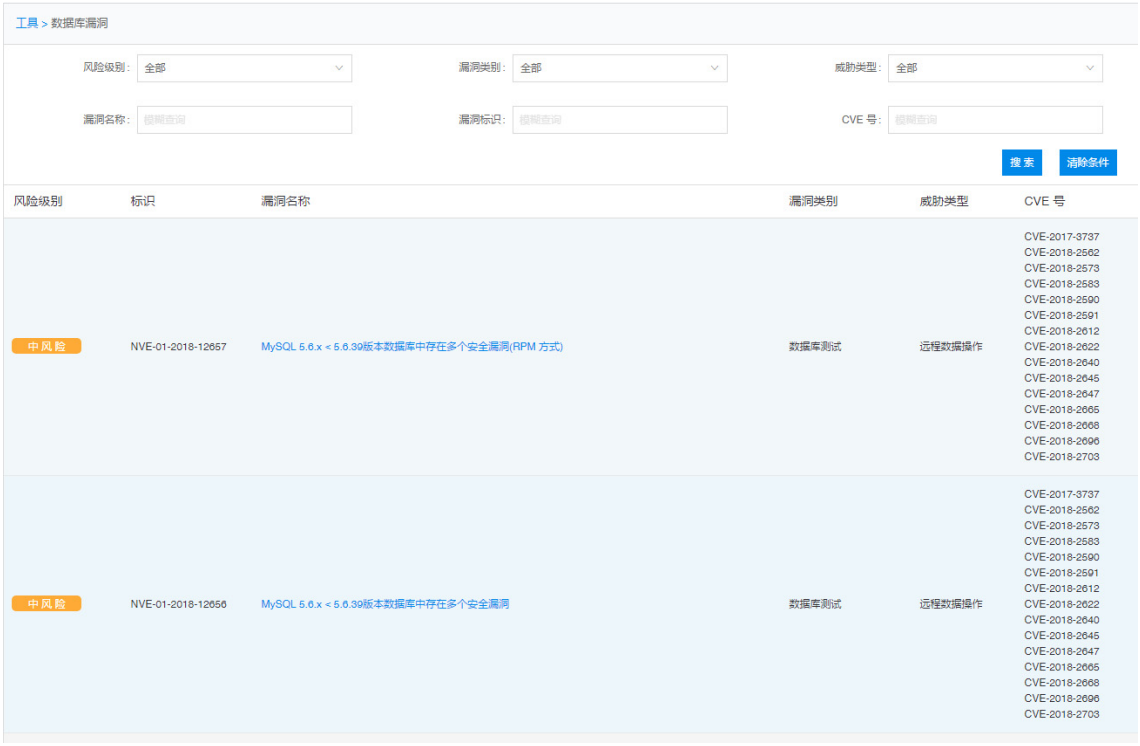
图6-3 知识库-主机漏洞



主机漏洞知识库包括风险级别、内部漏洞标识、漏洞名称、漏洞类别、威胁类型、CVE 号等知识，方便管理员对相关漏洞知识快速、全面了解。

6.1.3 数据库漏洞

图6-4 知识库-数据库漏洞



数据库漏洞知识库包括风险级别、内部漏洞标识、漏洞名称、漏洞类别、威胁类型、CVE 号等知识，方便管理员对相关漏洞知识快速、全面了解。

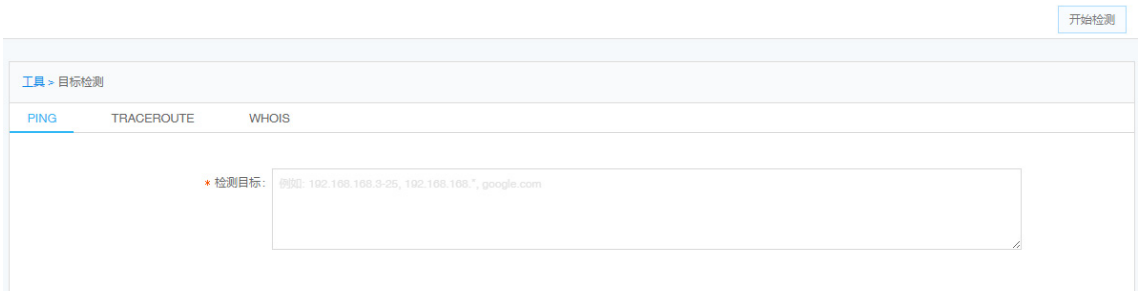
6.2 常用工具

6.2.1 目标检测

功能描述：ping\traceroute\whois 等常用目标检测工具。

配置路径：【工具】>【常用工具】>【目标检测】如下图所示。

图6-5 目标检测-PING



参数说明：

- <ping>：用于测试网络连接量的程序，用来检查网络是否通畅或者网络连接速度的命令。Ping 发送一个 ICMP(Internet Control Messages Protocol）即因特网信报控制协议；回声请求消息给目的地并报告是否收到所希望的 ICMP echo （ICMP 回声应答）。支持 IP、域名检测，点击<开始检测>通过 ping 回显结果可以检测目标设备是否在线。
- <TRACEROUTE>：用于测试源地址到达目标地址的路径及时间。在检测目标中输入目标 IP 或者域名，点击<开始检测>即可。
- <WHOIS>：可以查询域名是否已经被注册，以及注册域名的详细信息（如域名所有人、域名注册商、域名注册日期和过期日期等）。在检测目标输入框内输入单个 IP 或者域名，点击<开始检测>即可以查询域名归属者联系方式，以及注册和到期时间等信息。

6.2.2 端口扫描

功能描述：TCP、UDP 端口扫描工具。

配置路径：【工具】>【常用工具】>【端口扫描】如下图所示。

图6-6 端口扫描配置

参数说明：

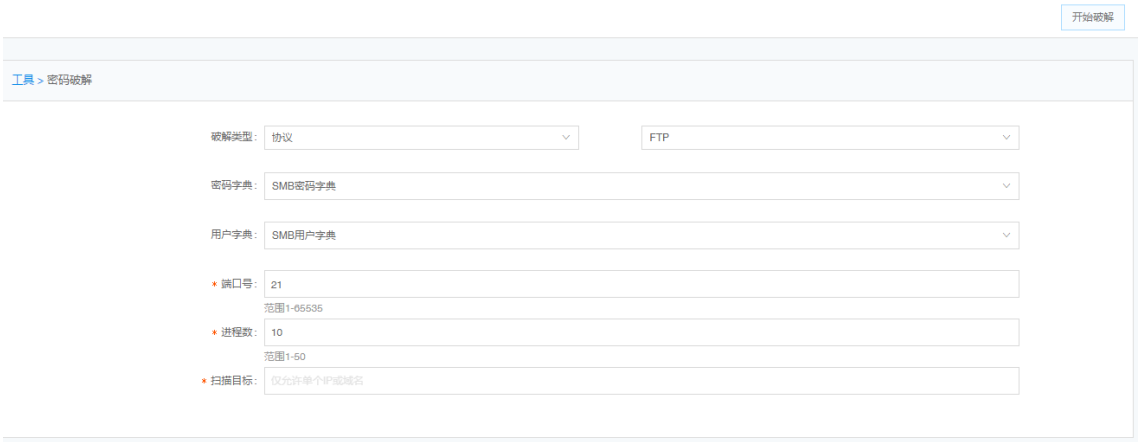
- <扫描类型>：包括 TCP、UDP、TCP＋UDP、SYN、FIN、ACK 等。其中，TCP 指采用全连接的方式扫描 TCP 端口；UDP 指只扫描 UDP 端口；TCP+UDP 指同时扫描 TCP 和 UDP 端口；SYN 指通过发送 SYN 包，采用半连接的方式扫描 TCP 端口；FIN 指通过发送 FIN 包，采用隐蔽的方式扫描 TCP 端口；ACK 扫描用于发现防火墙规则，确定它们是有状态的还是无状态的，哪些端口是被过滤的。
- <端口范围>：包括典型、全部和用户指定范围，如“1-2000”，“25，80，443”。
- <扫描目标>：输入框里输入目标 IP 地址，可以选择是单 IP、IP 段也可以是域名。
- <开始扫描>：点击<开始扫描>系统将按照端口扫描选项设置来检测出指定 IP 中端口开放信息。

6.2.3 密码破解

功能描述：FTP、SMB、RDP、VNC、SSH 和 TELENT 协议、以及数据库等密码破解。

配置路径：【工具】>【常用工具】>【密码破解】如下图所示。

图6-7 密码破解设置



参数说明：

- <破解类型>：支持协议（SMB、FTP、SSH、RDP、VNC、TELNET）和数据库服务（SQLSERVER、MYSQL）。
- <密码字典>：是用于破解的密码字典。
- <用户字典>：用于破解的用户字典。
- <端口号>：为破解的服务所使用的端口号，可以自行修改。
- <进程数>：执行破解的进程数。
- <开始破解>：点击<开始破解>，系统开始对检测目标进行密码破解。

6.2.4 加解密

功能描述：为用户提供加解密工具，类型包括文字加解密、MD5 加密、SHA1 加密、Base64 加解密

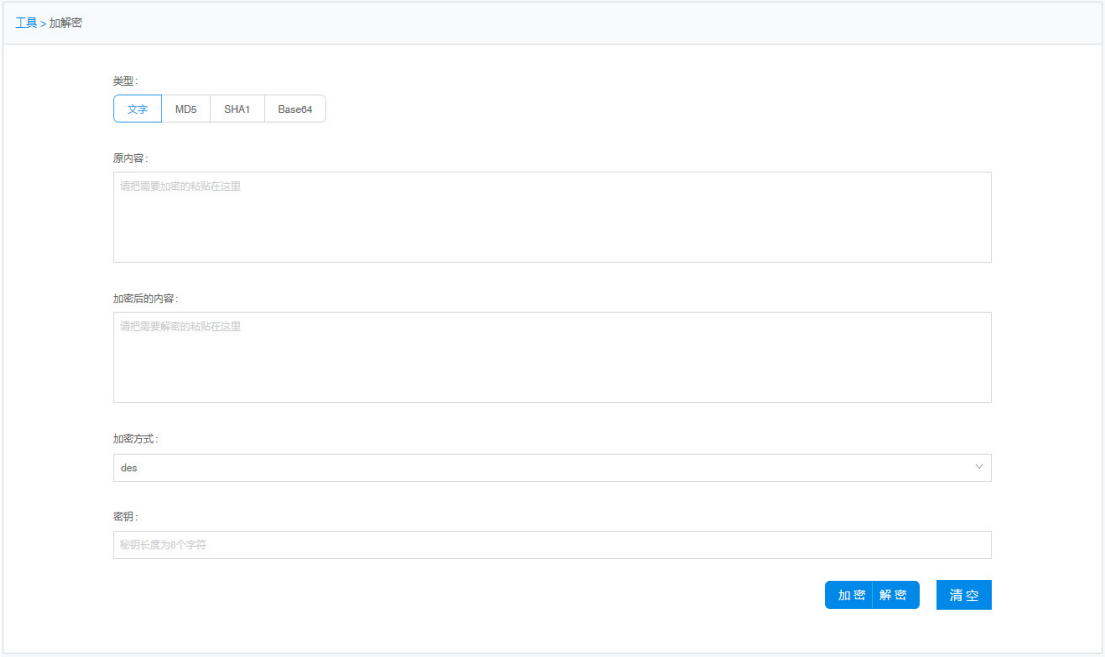
配置路径：【工具】>【常用工具】>【加解密】

1. 文字加解密

功能描述：提供文字内容的加解密，加密方式支持：des、3des、aes

配置路径：【工具】>【常用工具】>【加解密】，如下图所示。

图6-8 加解密工具-文字加解密



参数说明：

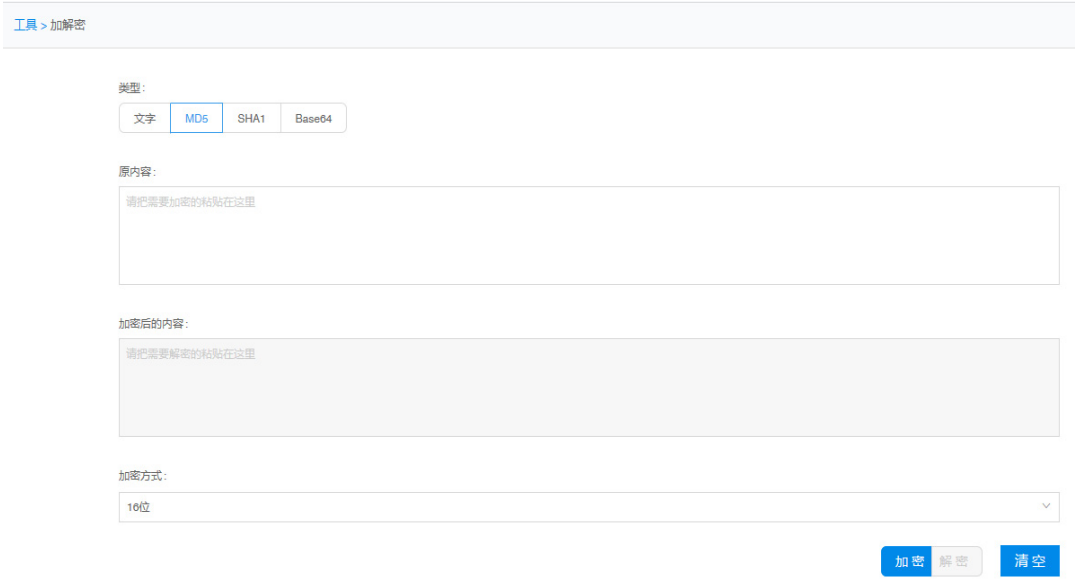
- <加密方式>：支持 des、3des、aes 三种加密方式。
- <加密>：在【原内容】输入框中输入要加密的内容，选择加密方式，输入密钥，点击【加密】，加密后的内容显示在【加密后的内容】文本框中。
- <解密>：在【加密后的内容】文本框中输入已加密的内容，选择加密方式，输入加密时使用的密钥，点击【解密】，解密后的内容显示在【原内容】文本框中。
- <清空>：清空【原内容】、【加密后的内容】的内容。

2. MD5 加密

功能描述：提供 MD5 加密工具，加密方式支持：16 位及 32 位

配置路径：【工具】>【常用工具】>【加解密】，如下图所示。

图6-9 加解密工具-MD5 加密



参数说明：

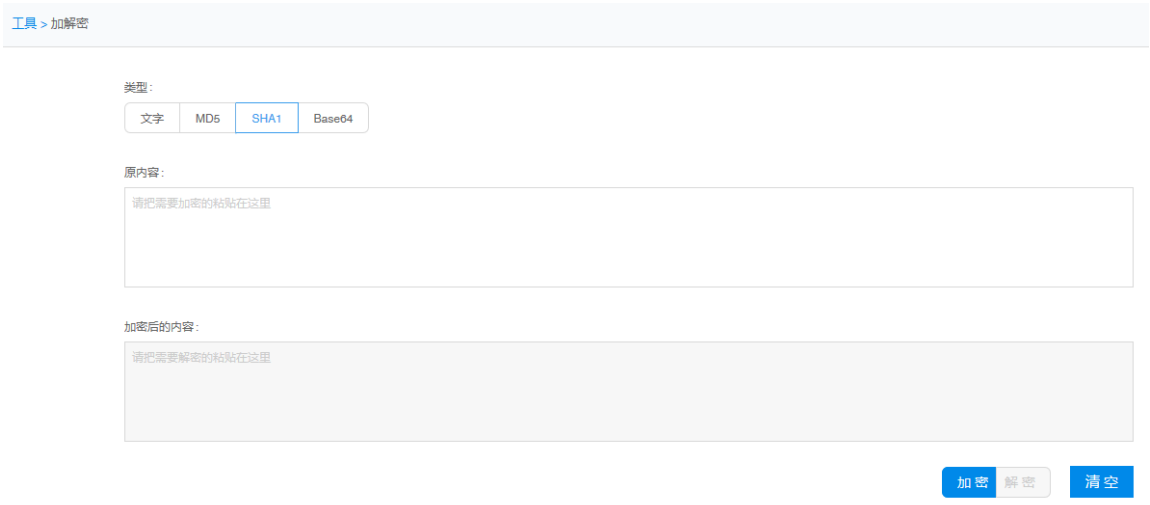
- <加密方式>：支持 MD5 16 位及 32 位加密。
- <加密>：在【原内容】输入框中输入要加密的内容，选择加密方式，点击【加密】，加密后的内容显示在【加密后的内容】文本框中。
- <清空>：清空【原内容】、【加密后的内容】的内容。

3. SHA1 加密

功能描述：提供 SHA1 加密工具。

配置路径：【工具】>【常用工具】>【加解密】，如下图所示。

图6-10 加解密工具-SHA1 加密



参数说明：

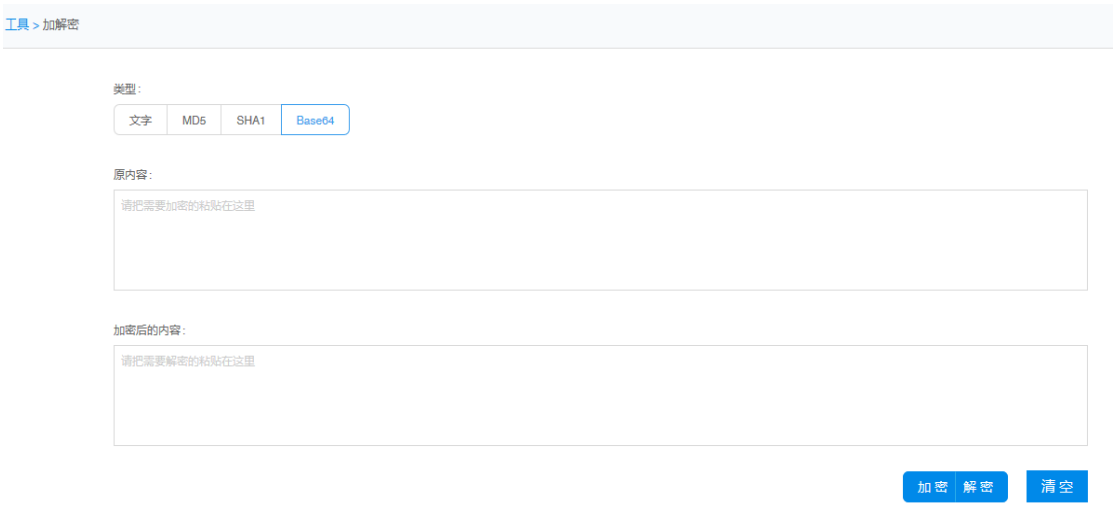
- <加密>：在【原内容】输入框中输入要加密的内容，选择加密方式，点击【加密】，加密后的内容显示在【加密后的内容】文本框中。
- <清空>：清空【原内容】、【加密后的内容】的内容。

4. BASE64 加解密

功能描述：提供 BASE64 加解密工具。

配置路径：【工具】>【常用工具】>【加解密】，如下图所示。

图6-11 加解密工具-BASE 64 加解密



参数说明：

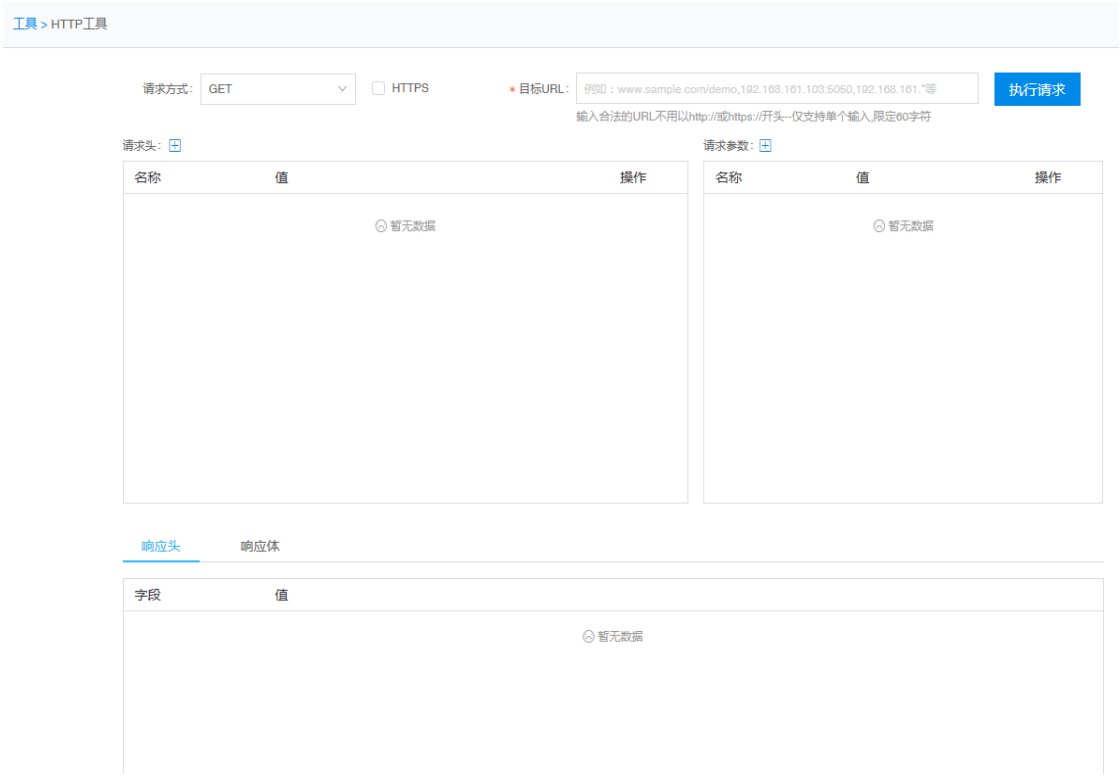
- <加密>：在【原内容】输入框中输入要加密的内容，点击【加密】，加密后的内容显示在【加密后的内容】文本框中。
- <解密>：在【加密后的内容】文本框中输入已加密的内容，点击【解密】，解密后的内容显示在【原内容】文本框中。
- <清空>：清空【原内容】、【加密后的内容】的内容。

6.2.5 HTTP工具

功能描述：提供 HTTP 工具供用户对扫描的网站进行测试。

配置路径：【工具】>【常用工具】>【HTTP 工具】如下图所示。

图6-12 HTTP 工具



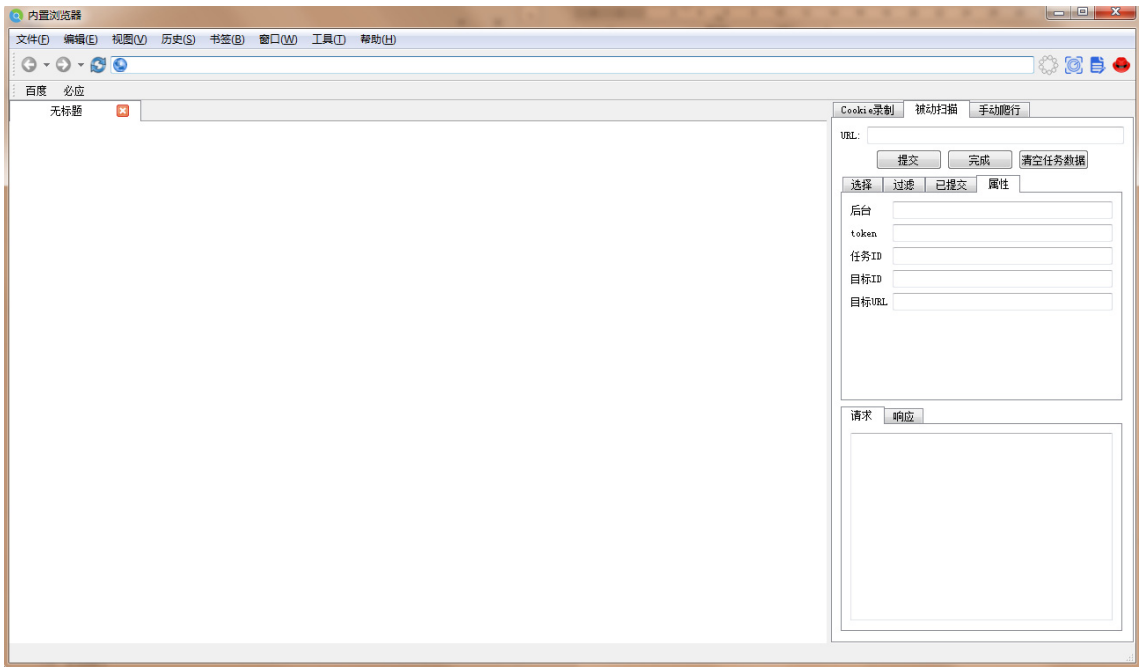
参数说明：

- <请求方式>：支持多种 http 请求方式，提供 GET、POST、HEAD、POST、PUT、DELETE、OPTIONS、TRACE 八种请求方式。
- <目标 URL>：输入要测试的目标网站 URL，不需要以 http://或 https://开头。
- <请求头>：输入键值对形式的请求头参数，伴随请求发送给目标网站。
- <请求参数>：输入目标网站需要的参数值，伴随请求发送给目标网站。
- <执行请求>：点击执行请求，以选中的请求方式进行访问目标网站。
- <响应头>：目标网站接收到请求返回的响应头，有目标网站的一些基本信息。
- <响应体>：目标网站收到请求返回的响应体，例如网页源码。

7 系统专用浏览器

7.1 页面功能介绍

图7-1 系统专用浏览器



7.1.2 标题栏

- 最小化按钮：最小化到托盘
- 最大化：窗口最大化拉伸
- 关闭：关闭窗口，第一个提示是选择是否最小化，第二个提示是说明关闭的影响，第三个是提示多个标签打开时是否确认关闭。

7.1.3 菜单栏

1. 文件

图7-2 文件

2. 编辑

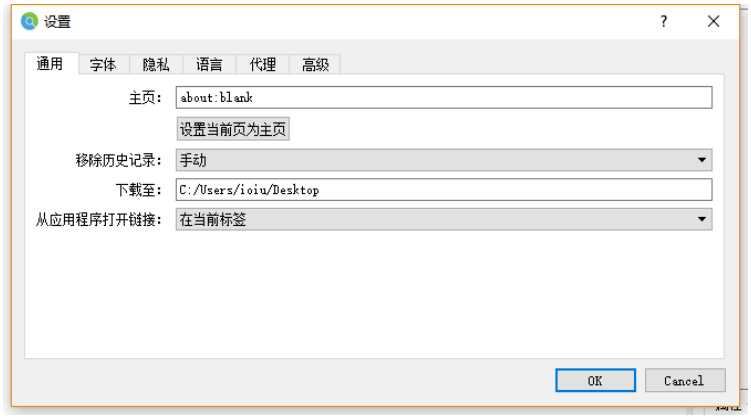
图7-3 编辑

3. 设置

- 通用

  可以在此处设置主页、清除历史记录的周期、文件下载保存路径、如何处理链接。

图7-4 通用



- 字体

  字体分为标准字体和等宽字体，此处只是设置默认值。

图7-5 字体

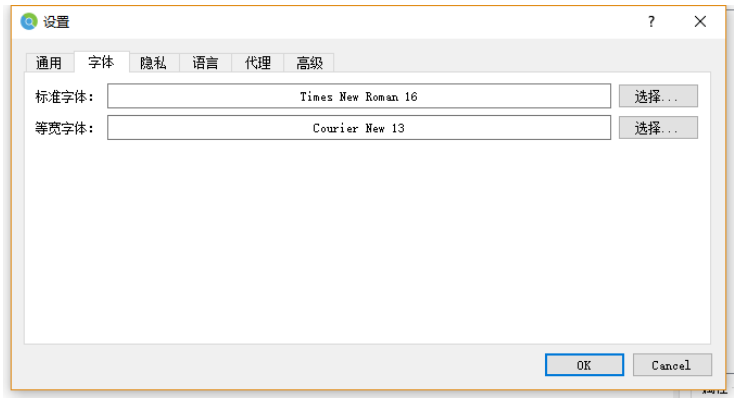
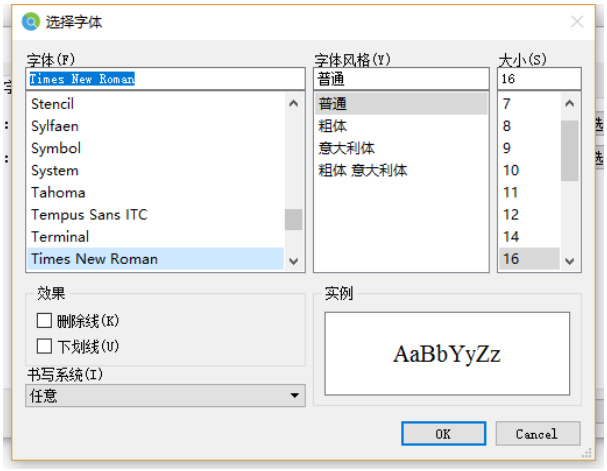


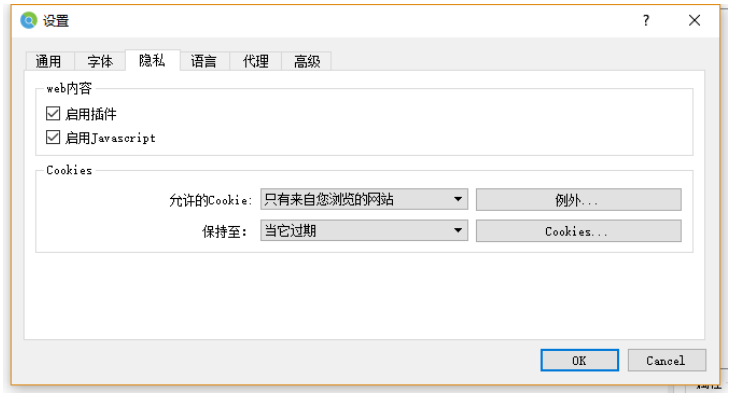
图7-6 字体



- 隐私

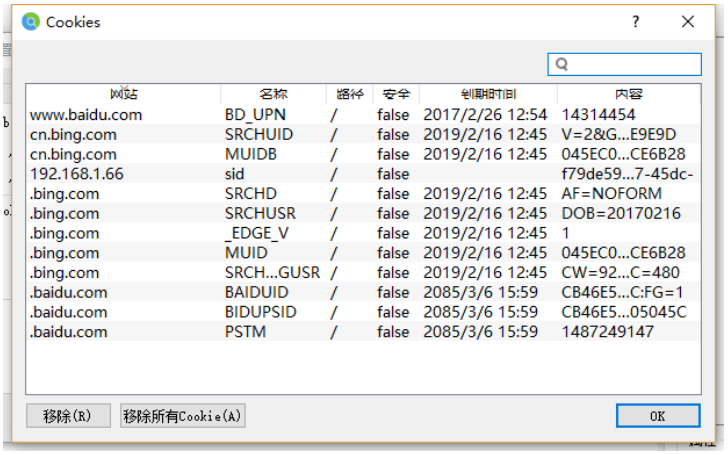
  此处设置包括启用插件、JavaScript 执行、Cookie 管理等。

图7-7 隐私



- Cookie 管理

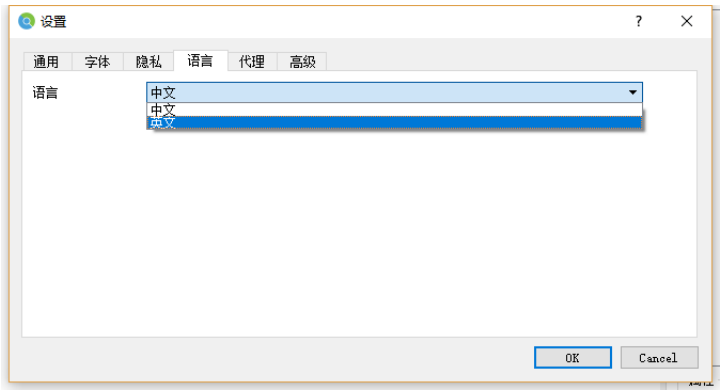
图7-8 Cookie 管理



- 语言

  暂只支持中文和英文。

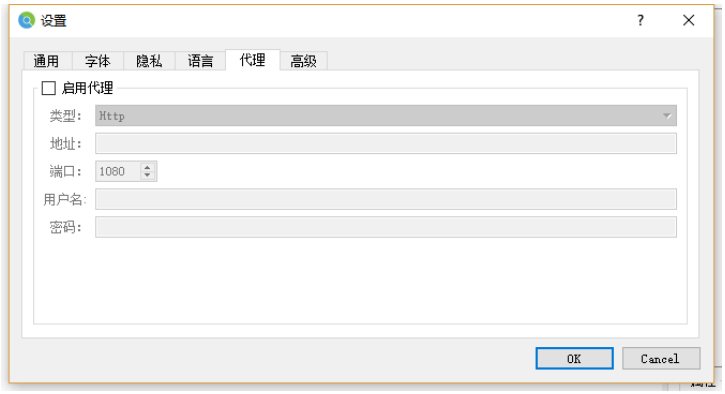
图7-9 语言



- 代理

  网络代理参数设置处，支持 http 和 socks5 代理。

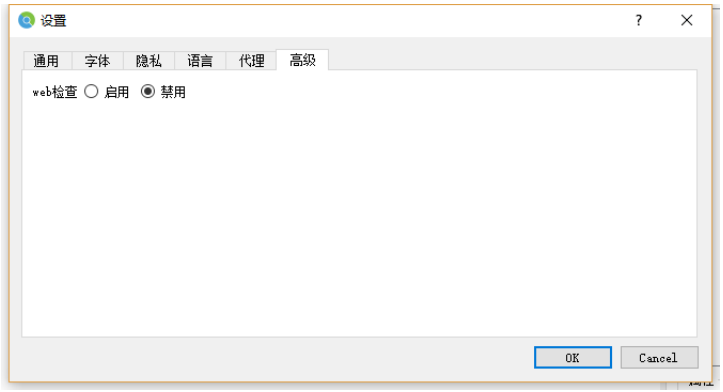
图7-10 代理



- 高级

  启用 web 检查，默认为禁用，若启用，将在网页右键菜单中看到选项入口。

图7-11 高级

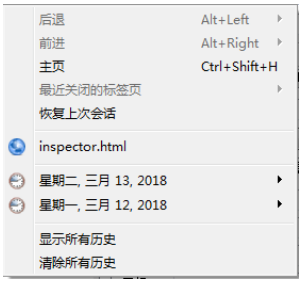


- 视图

图7-12 视图

- 历史

图7-13 历史

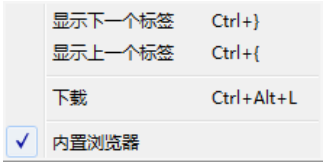


- 书签

图7-14 书签

- 窗口

图7-15 窗口

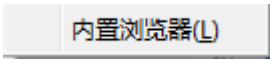


- 工具

图7-16 工具

- 帮助

图7-17 帮助



7.1.4 导航栏

- 前进按钮，包含前进历史。
- 后退按钮，包含后退历史。
- 刷新，重新加载。
- URL 地址栏，包含背景颜色进度条，自动补全功能。
- 加载动态图，标示加载过程。
- 工具集显示切换开关。
- 菜单栏切换显示开关：若菜单栏被隐藏时相关快捷键将失效。
- 渗透测试工具入口。

图7-18 导航栏

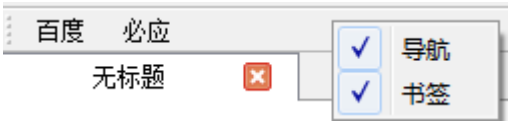
提示

请不要隐藏导航栏。

7.1.5 书签栏

显示工具栏书签，可以隐藏条目（右键单击工具栏以选择关闭）。

图7-19 书签栏



7.2 Cookie录制

红色条目表示会话 Cookie，在关闭浏览器里此类 Cookie 将会被删除。若使用了 Cookie 录制且存在会话 Cookie，在任务结束前，最好不要关闭浏览器和相关标签页，关闭可能会产生不可预估的结果。

点击<完成并复制>会将 Cookie 以特定的格式复制到剪切板，在漏洞扫描系统创建任务的地方粘贴即可。

图7-20 Cookie 录制

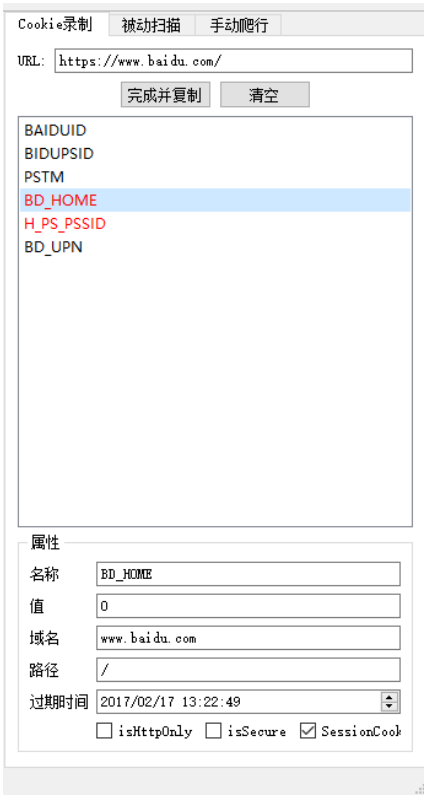
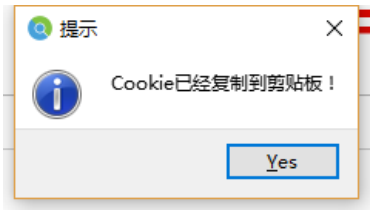


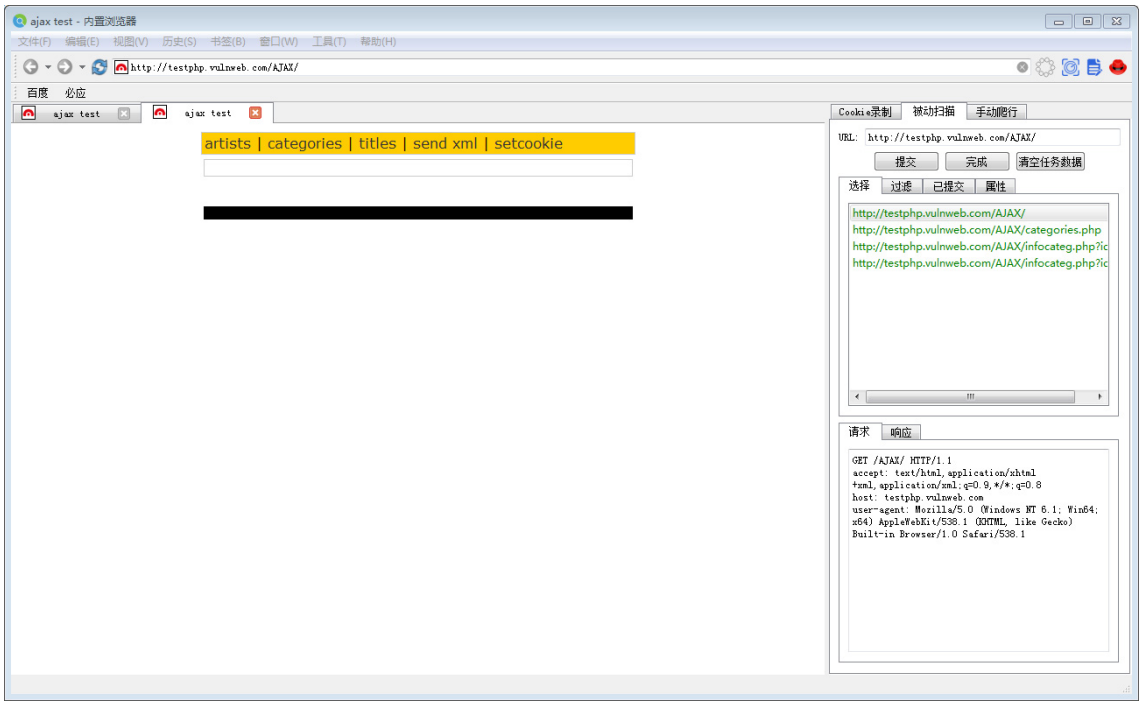
图7-21 Cookie 录制



7.3 被动扫描

工具会监视剪切板，若匹配到预先定义好格式的链接，会自动开启被扫描任务，也只能通过预先定义好格式的链接来创建任务。若要对网一个网站进行多次被动扫描，需要点击<清空任务数据>清空上一个任务的数据后才能继续进行。数据可以在中间进行多次提交，但在任务的最后，需要点击<完成>以提交最后的数据并标志结束。

图7-22 被动扫描



过滤的请求：通过匹配响应数据的 Content-Type 字段内容来过滤，而不是请求 url 的扩展名，若为 CSS、图片、音频、或视频等数据，则默认添加到【过滤】的数据中，当然，可以将过滤的数据移动到【选择】中去，通过右键菜单。

图7-23 过滤

提交数据成功时，数据会移动到【已提交之中】。

【属性】标签页放置后台 URL、token、任务 ID 等数据。

【请求】和【响应】用于显示每一个请求的原始报文内容。

图7-24 请求

图7-25 响应

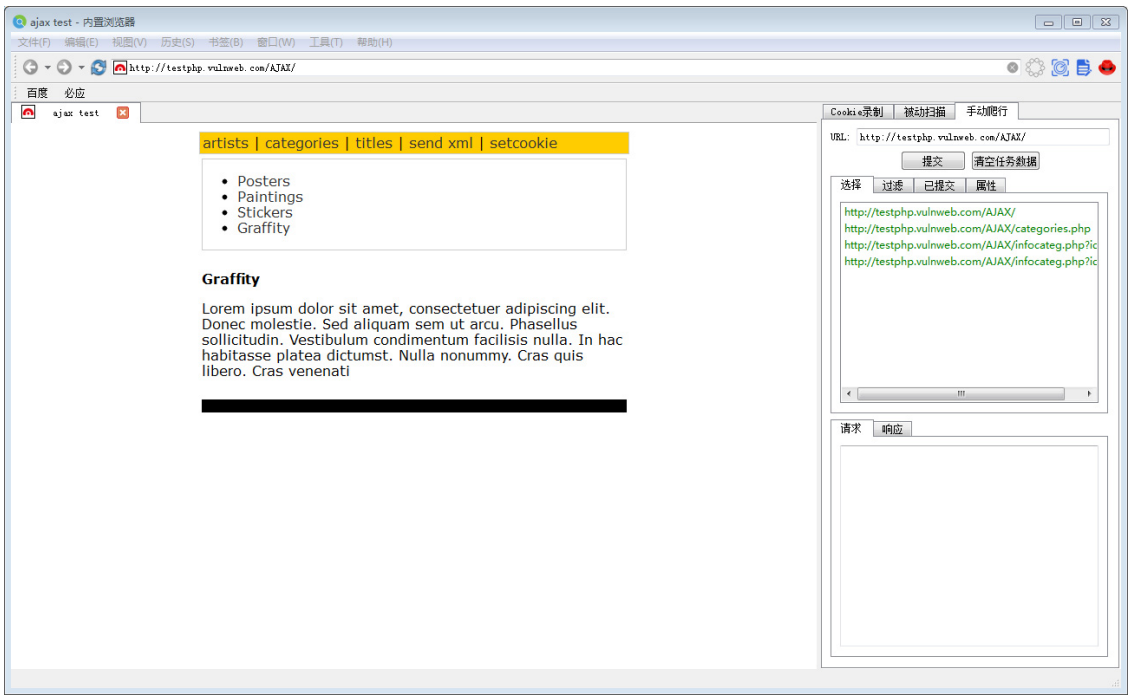
7.4 手动爬行

手动扫描是用户通过手动点击浏览器浏览 web 页面，扫描器会把符合项目扫描参数配置的 URL 添加到已扫描到的 URL 列表中。

新建子任务，执行计划选择<暂不执行>，扫描类型选择<主动扫描>，点击子任务【操作】栏目下的

，弹出手动爬行列表，下载手动爬行工具，根据提示复制 URI，打开专用浏览器界面，点击浏览器里的 URL 链接。

图7-26 手动爬行



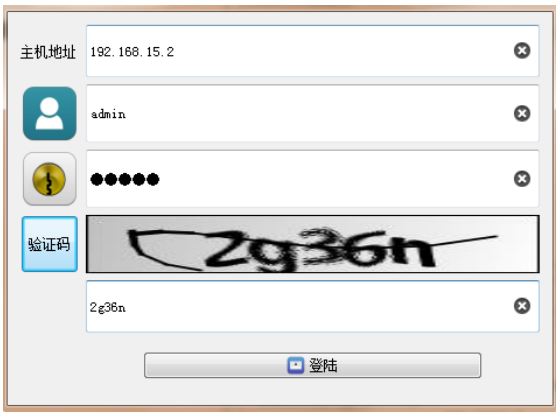
URL 链接会自动保存到爬行到的 URL 列表中。同被动扫描功能，唯一不同的地方是它只作为爬虫的一个补充。

7.5 渗透测试

打开方式：单击  打开，或通过菜单栏（【工具】->【渗透测试】），或快捷键（Ctrl + Y）

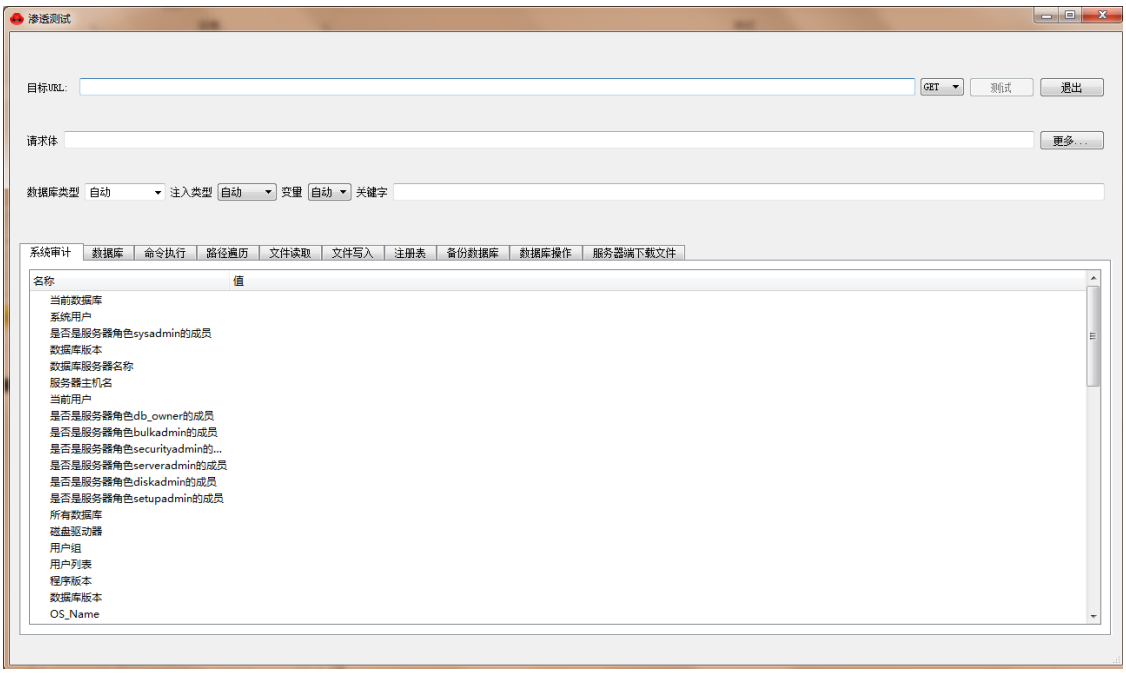
使用此模块需要进行相关验证，如下图。

图7-27 登录窗口



主机地址填写漏洞扫描系统的 IP（不需要填写端口号），再填写用户名、密码，点击“验证码”刷新验证码，输入验证码后，点击“登陆”进行验证，若验证通过将打开渗透测试模块，每一次打开都需要进行验证，您所登陆的信息不会作任何记录，防止关键信息泄漏。渗透测试具有一定的风险性，应当根据情况选择合适的时机运行，选取不同的 URL 对渗透的结果影响很大，在同等情况下，优先选择连接数据库权限较高者。

图7-28 主界面：



主要功能模块包括系统审计、数据库、命令执行、路径遍历、文件读取、文件写入、注册表、备份数据库、数据库操作、服务器端文件下载等。不同的数据库有的功能模块不一样多。在没有检测到渗透变量的时候，上述功能将不作为。

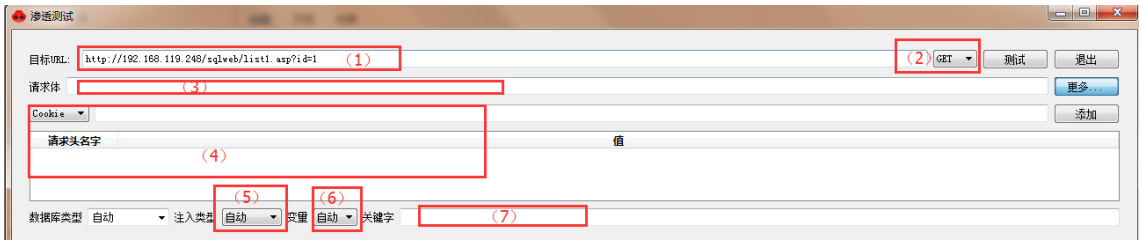
以 MSSQL 为例进行说明：

1. 输入相关数据

相关数据的填充可以通过从扫描结果里面复制渗透测试链接进行自动填充（数据复制到剪切板时会被检测到）。当然相关数据也可以手动输入。

默认情况下显示简单输入数据点，点击“更多”显示全部输入数据。

图7-29 渗透工具



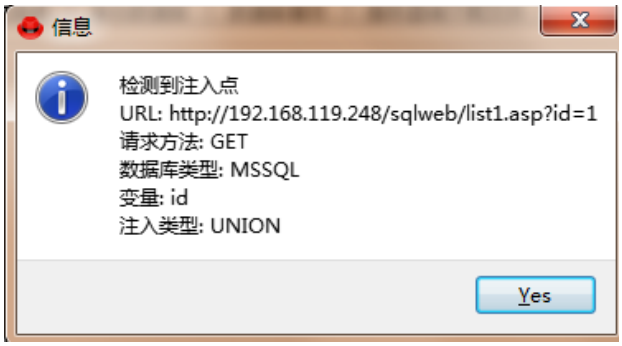
- 标识 1：URL 地址输入点。
- 标识 2：URL 的请求方法，支持 GET、POST，暂不支持自定义。
- 标识 3：请求体输入，若存在请求体，将不检测 URL 的查询变量，只检测请求体变量。
- 标识 4：自定义请求头，暂只支持输入 Cookie 和 Referer 头，输入后点击“添加”来添加到表格。
- 标识 5：注入类型，若知道注入类型，可以手动指定，否则默认自动。支持布尔、时间、堆栈、错误、联合注入检测。注意：数据库类型暂不支持指定。
- 标识 6：指定需要检测的变量名，默认自动。
- 标识 7：指定关键字，此关键字只存在于正常页面而不存在于注入页面。默认为空时，自动提取关键字。

2. 点击<测试>

测试过程可能需要花费较长时间，由网络状态、请求个数、Payload 数量等多个因素共同决定。

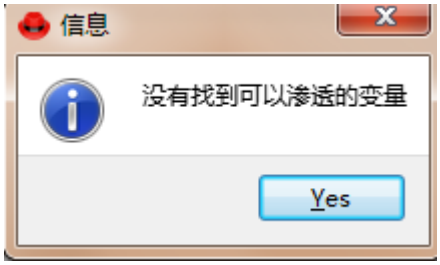
存在注入点时，将会有提示。

图7-30 提示信息



没有检测到可渗透的变量时提示。

图7-31 提示信息

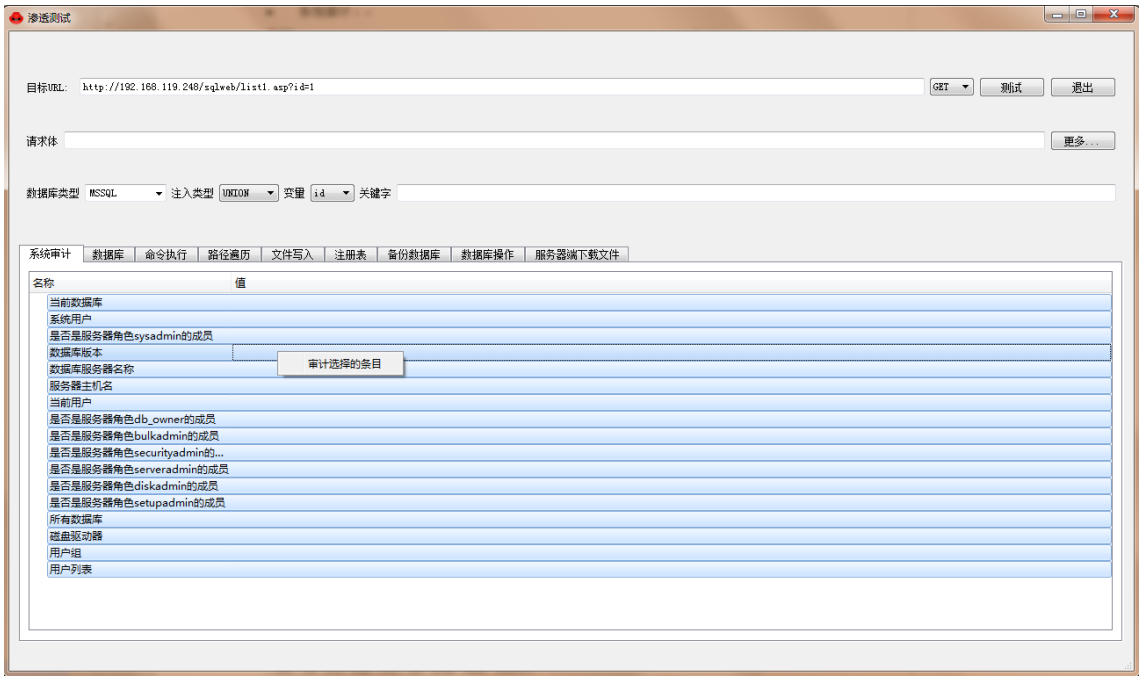


若注入成功，将根据数据库选择相应的功能模块。

3. 相关功能测试

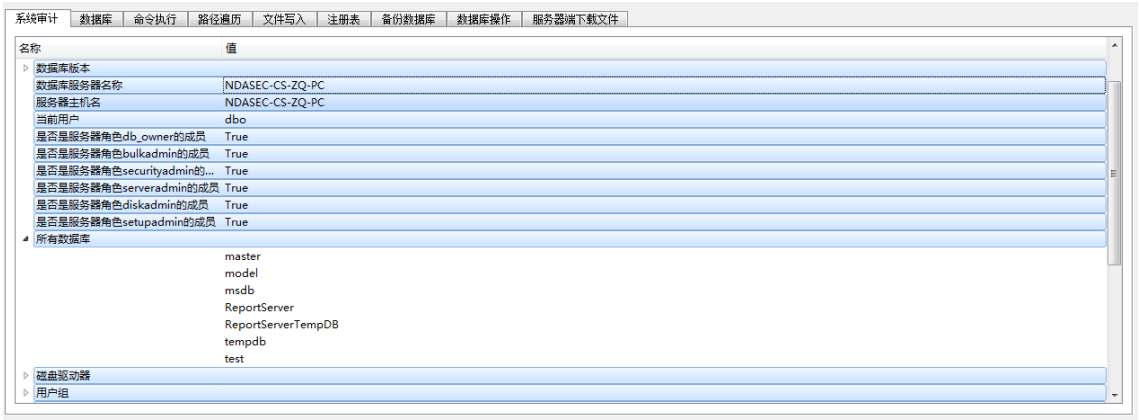
- 系统审计

图7-32 系统审计



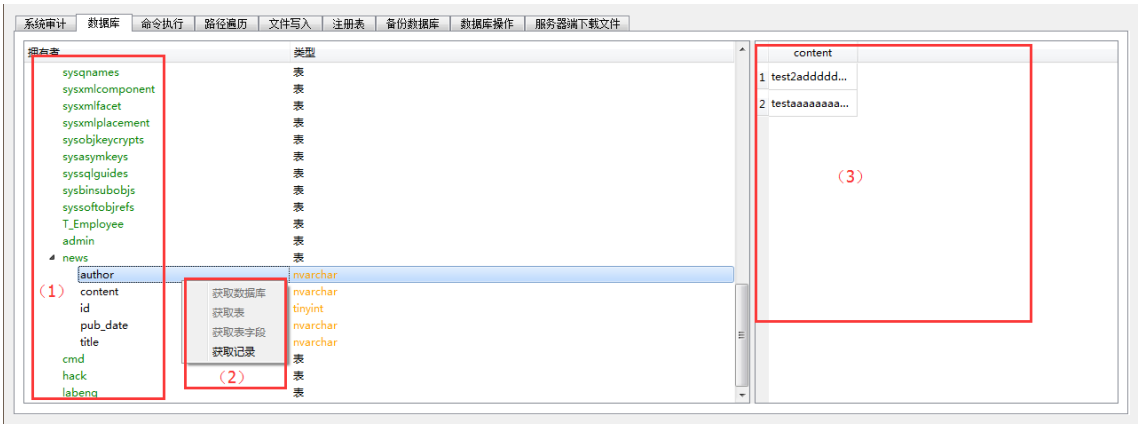
通过鼠标框选相应的条目，右键菜单选择审计即可得到结果。也可对单个条目进行审计，不同数据库的审计条目不一致。审计结果受目标数据库的配置、权限影响。

图7-33 系统审计



- 数据库

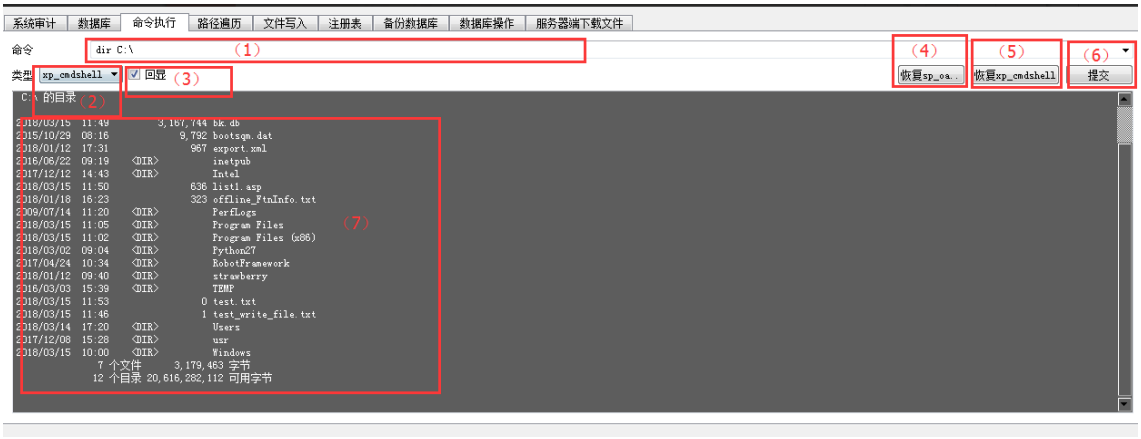
图7-34 数据库



通过右键菜单进行操作，使用框选来选择获取哪些条目。

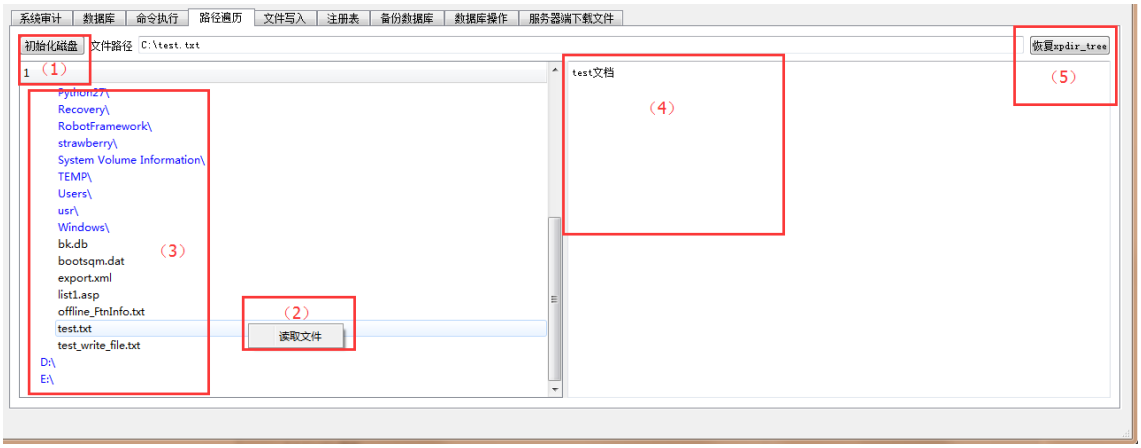
- 标识 1：数据库树结构
- 标识 2：右键菜单，选择不同内容会有相应的选项
- 标识 3：获取结果的表数据内容
- 命令执行

图7-35 命令执行



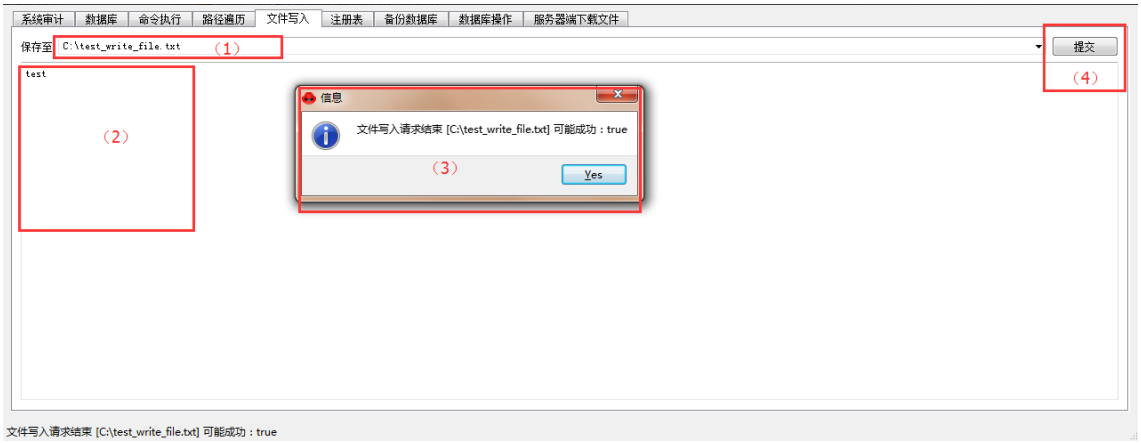
- 标识 1：命令输入框，输入后的命令会加入列表框中。
- 标识 2：命令执行类型，暂只支持 xp_cmdshell。
- 标识 3：是否开启回显，该功能可能会影响使用的 payload。
- 标识 4：恢复 sp_oa 权限。某些数据库不能执行命令，需要先执行此项操作。
- 标识 5：恢复 xp_cmdshell 权限。某些数据库不能执行命令，需要先执行此项操作。
- 标识 6：提交命令执行请求。
- 标识 7：显示命令执行结果。
- 路径遍历

图7-36 路径遍历



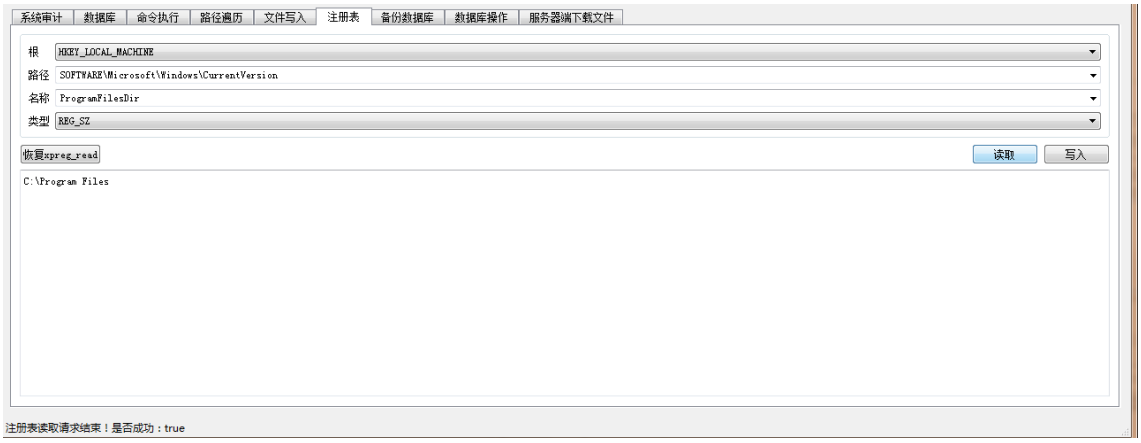
- 标识 1：初始化磁盘。获取盘符，比如 C、D 盘。
- 标识 2：右键菜单。点击目标和文件时会有相应的功能，如文件夹时为获取子文件夹，文件时为读取文件。
- 标识 3：磁盘目录树结构。
- 标识 4：读取的文件内容展示点。
- 标识 5：恢复 xpdir_tree。某些数据库不能执行路径遍历，需要先执行此项操作。
- 文件写入

图7-37 文件写入



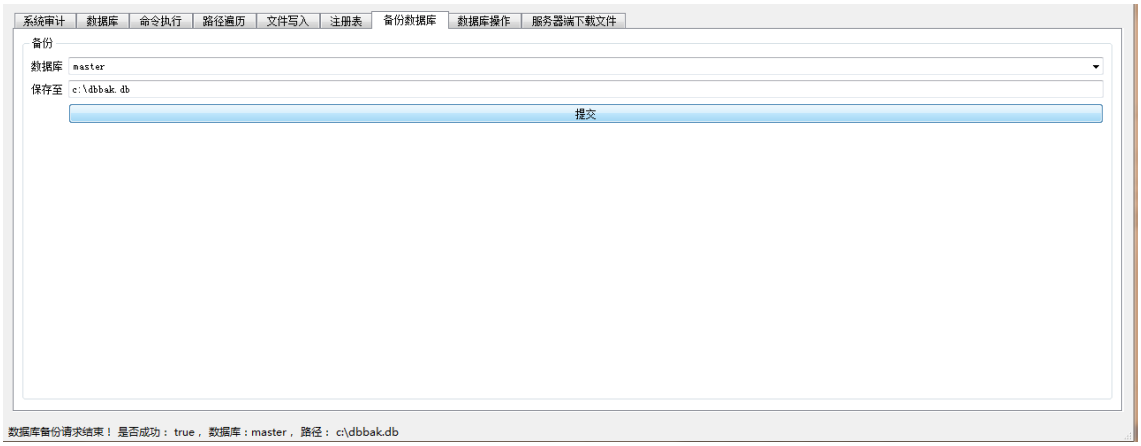
- 标识 1：写入文件的路径，请不要带中文或空格。
- 标识 2：需要写入的文件内容。
- 标识 3：请求结束时的弹窗说明。
- 标识 4：提交写文件请求。
- 注册表

图7-38 注册表



- 备份数据库

图7-39 备份数据库



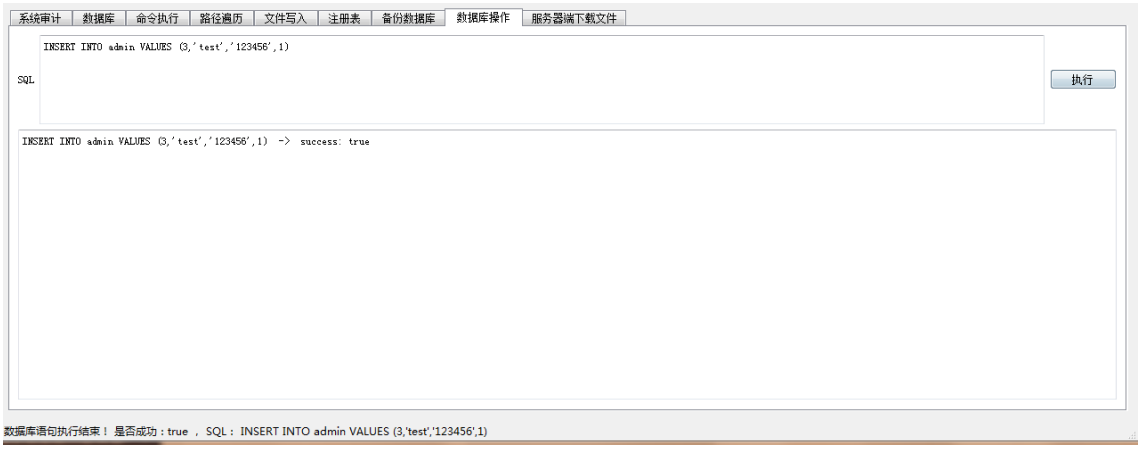
- 数据库操作

在数据库表操作测试页面用户可以尝试进行对 web 应用数据库表进行操作的测试。

在该测试中可进行创建表、插入记录、更新记录、删除记录、删除表的操作测试。

首先，选择命令关键字，输入要操作的表名和相应的 SQL 语句，点击<执行>按钮开始执行 SQL 语句，执行成功后该页面如图：

图7-40 数据库操作



- 服务器端下载文件

在正确配置好基础参数部分的各个选项后，在远程下载测试页面用户可以尝试进行对 web 应用服务器文件目录中下载文件的测试。

首先，在目标 URL 输入框输入要下载的文件 URL 地址，在保存至服务器文本框输入要下载到 web 应用服务器上的目录及文件名后，点击开始按钮执行远程下载测试，测试完成后页面如图：

图7-41 服务器端下载文件