铱迅漏洞扫描系统

管理员手册

南京铱迅信息技术股份有限公司

Nanjing YXLink Information Technology Co., Ltd.

未经南京铱迅信息技术股份有限公司（Nanjing YXLink Information Technology Co.,Ltd.，简称：铱迅信息）的事先书面许可，对本产品附属的相关手册之所有内容，不得以任何方式进行翻版、传播、转录或存储在可检索系统内，或者翻译成其他语言。

- 本手册没有任何形式的担保、立场表达或其他暗示。若有任何因本手册或其所提到之产品信息，所引起直接或间接的数据流失、利益损失或事业终止，铱迅信息不承担任何责任。
- 铱迅信息保留可随时更改手册内所记载之硬件及软件规格的权利，而无须事先通知。
- 本手册描述的“铱迅漏洞扫描系统”之所有功能，并非所有型号都支持，对于每个型号拥有的功能模块，请咨询供货商或联系铱迅客服人员。
- 本公司已竭尽全力来确保手册内载信息的准确性和完善性。如果您发现任何错误或遗漏，请向铱迅信息反映。对此，我们深表感谢。

商标信息

铱迅信息、铱迅信息的标志、铱迅漏洞扫描系统的标志为南京铱迅信息技术股份有限公司的商标或注册商标。本手册或随铱迅信息产品所附的其他文件中所提及的所有其他商标名称，分别为其相关所有者所持有的商标或注册商标。

版本历史

版本	发布时间	说明
0.9	2011 年 10 月 12 日	初稿
1.0	2011 年 11 月 20 日	细化功能描述
4.1	2016 年 11 月 18 号	更新部分文字
4.2	2019 年 10 月 22 号	更换产品 logo 和截图

阅读指导

如果您是第一次使用铱迅漏洞扫描系统，建议首先阅读如下章节：

安装及初始化

快速使用指南

开始使用

如果您做日常扫描任务分析和查看，建议阅读如下章节：

状态

漏洞扫描

报表管理

如果您是高级用户，建议重点阅读如下章节：

参数配置

网络配置

系统

日志

Console 口

复位和还原

如果您想了解产品特点及规格，建议阅读如下章节：

简介

产品规格

如果您有问题需要寻求答案，可阅读如下章节：

常见问题与解答

目　录

前言

文档范围

本文将覆盖铱迅漏洞扫描系统的硬件产品规格和 Web 管理界面的所有功能特点，并详细介绍该系统的具体使用方法。

期望读者

期望了解本产品主要技术特性和使用方法的系统管理员、网络管理员、网络安全专家等。本文假设您对下面的知识有一定的了解：

- 系统管理
- TCP/IP 协议
- HTTP 协议
- Windows 或 Linux 操作系统

内容简介

1. 简介：介绍铱迅漏洞扫描系统的产品功能
2. 产品规格：介绍本产品的硬件规格和电气特性
3. 安装部署：简明介绍本产品的安装和部署方式
4. 安装及初始化：介绍本产品的安装的一般过程
5. 快速使用指南：介绍设备的基本使用方法
6. 开始使用：介绍 Web 管理页面的内容组织和使用指南
7. 状态：介绍 Web 管理界面中的设备基本信息的查看
8. 漏洞扫描：介绍 Web 管理界面中的漏洞扫描功能
9. 资产管理：介绍 Web 管理界面中的资产管理功能
10. 策略管理：介绍 Web 管理界面中的扫描策略
11. 报表：介绍 Web 管理界面中的报表功能
12. 网络配置：介绍 Web 管理界面中的网络接口设置
13. 参数配置：介绍 Web 管理界面中相关参数的设置
14. 系统：介绍 Web 管理界面中的系统操作功能
15. 日志：介绍系统的日志导出与清理功能

16. Console 功能：介绍 Console 功能的配置

17. 系统复位与还原：系统的复位与还原的方法

18. 常见问题与解答：用户常见的问题与解答

附录 A：出厂默认设置

获得帮助

获取网络安全相关资料可以访问网站：http://www.yxlink.com

如需获取更详尽的网络安全服务信息、商务信息，您可通过如下方式和我们取得联系：

地址：江苏省南京市雨花台区宁双路 18 号沁恒科技园 D 幢 4 层

邮编：210012

服务热线：400-097-5577

电话：025-83235296，025-83235396，025-58722055

传真：025-83235296，025-83235396 转 601

网站：http://www.yxlink.com

Email：info@yxlink.com

格式与名词约定

设备、产品、系统、漏扫——除非特指，本手册中均表示铱迅漏洞扫描系统

【A】 —— 菜单名称和按钮名称的表示方式

【A】→【B】—— 菜单项选择的表示方式

—— 使用技巧、建议和引用信息等

—— 重要注意信息

1、简介

产品介绍

铱迅漏洞扫描系统（简称：YXLink NVS，英文：YXLink Network Vulnerability Scan System），是检查主机漏洞的专业扫描系统，是目前少数支持 IP 地址段批量反查域名、内网穿透扫描的专业漏洞扫描器，可支持主机漏洞扫描、Web 漏洞扫描、弱密码扫描等。主要产品功能有：

主机漏洞扫描：支持缓冲区溢出测试、网络设备测试、WEB 服务器测试、数据库服务器测试、邮件服务器测试、DNS 测试、系统测试等主机漏洞。

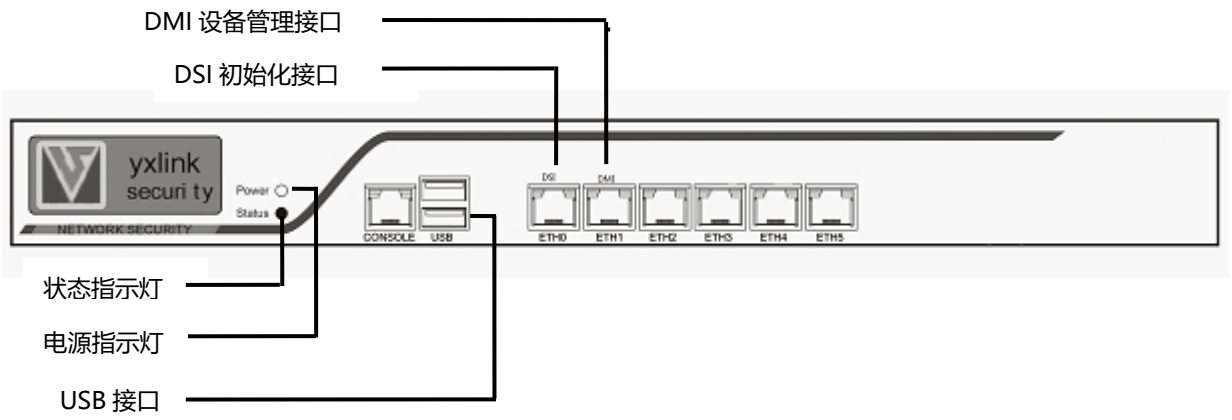
Web 扫描漏洞：支持 SQL 注入、跨站脚本、木马上传、代码执行、远程本地包含、信息泄露等 web 漏洞。

弱密码检测：支持 FTP，SSH，3389，TELNET，MSSQL，MYSQL，ORACLE，SMB，VNC 的弱密码检测，且提供弱密码字典的自定义。

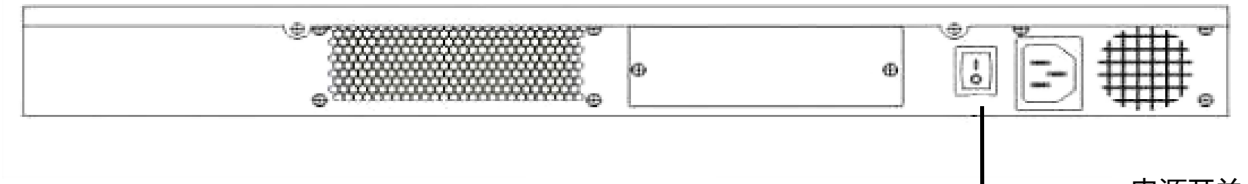
通过部署铱迅漏洞扫描系统，能够降低与缓解主机中的漏洞造成的威胁与损失，快速掌握主机和网络中存在的脆弱点。铱迅漏洞扫描系统可以广泛用于 Web 系统、电子商务、在线交易等平台。

2、产品规格

面板说明



面板



背板

接口说明

注意：

DSI 接口自带 DHCP 功能，仅供直接连接计算机时使用。

切勿将其接入内部管理网络，否则会造成 DHCP 冲突。

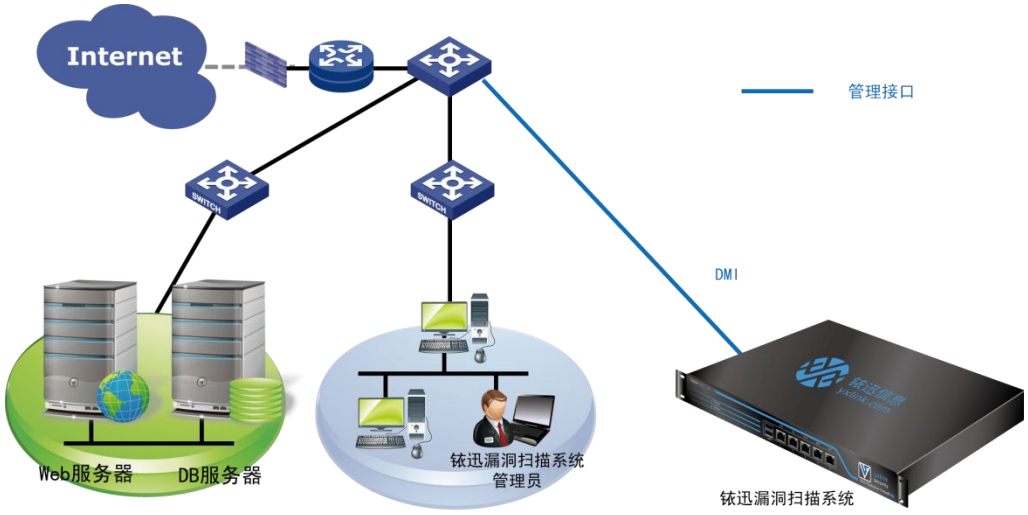
序号	名称	说明
1	Console 接口	Console 口可以对设备进行常用配置，特别是当设备无法通过 Web 方式进行正常的管理维护的时候，可以通过 Console 功能，对设备进行管理，查看设备的状态，对设备

		进行配置、复位或还原等操作。
2	DSI 接口	设备初始化管理接口(Device Setting Interface)，直接连接计算机，供本设备初次启动时配置 DMI 接口的 IP 地址使用。在正常情况下，此接口无需连接任何网络。
3	DMI 接口	设备管理接口(Device Management Interface)， 连接内部管理网络，管理员通过此接口登录本设备的 Web 管理页面进行日常管理工作。
4	电源指示灯	指示设备的电源状态，熄灭表示断电状态。
5	状态指示灯	指示设备的磁盘读写。闪烁时表示正在读写磁盘。
6	USB 接口	USB 接口，厂家检修使用或者用于产品复位。
7	电源开关	设备的电源开关。

3、安装部署

直接部署方式

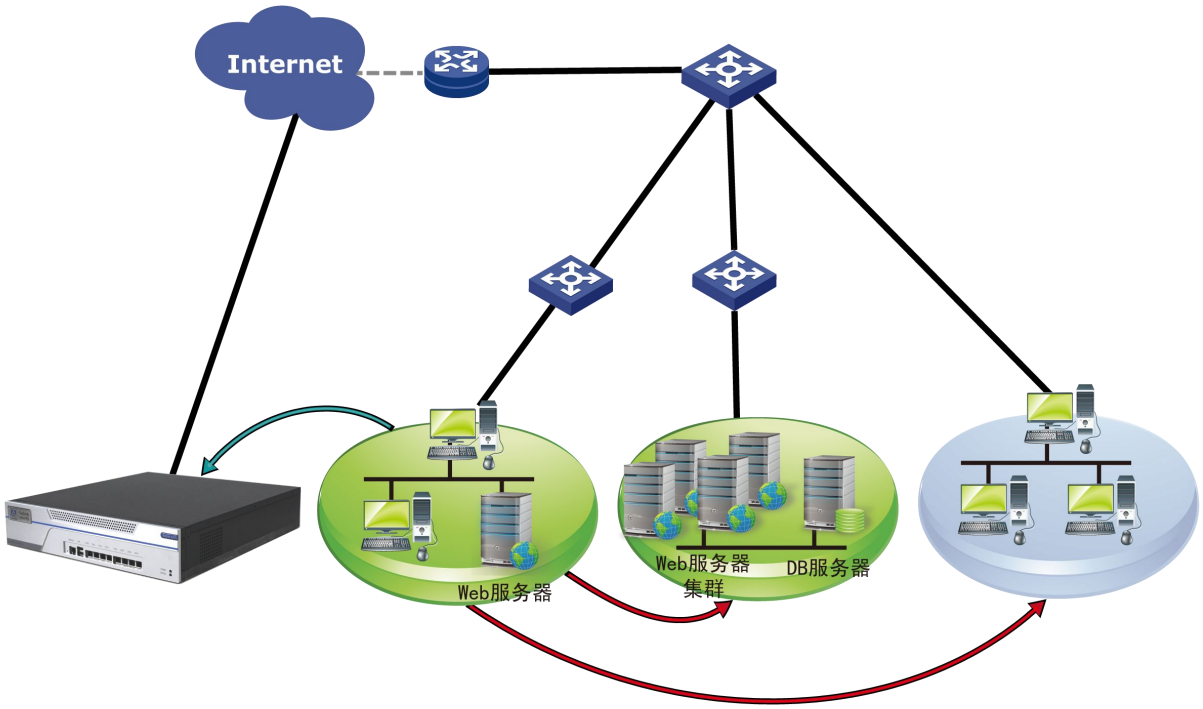
铱迅漏洞扫描系统，只要部署在任何网络可以到达的环境中就可以立即工作。



内网穿透扫描部署方式

铱迅漏洞扫描系统，不需要像传统漏洞扫描系统那样，必须在内网部署，才可以进行扫描内部网络。也可以只需要利用一台内网的跳板机器，安装上铱迅漏洞扫描系统的辅助软件，即可实现对内网所有机器的穿透扫描，也就是可以进行远程扫描。

只需要利用一台内网的跳板机器，即可进行远程扫描。


Internet
Web服务器
Web服务器
集群
DB服务器

4、安装及初始化

打开包装箱

对照物品清单检查物品，如果发现有所损坏或者任何配件短缺的情况，请及时和供货商联系。

安装设备

请使用附件箱中的耳片和螺钉将设备固定在机架上。

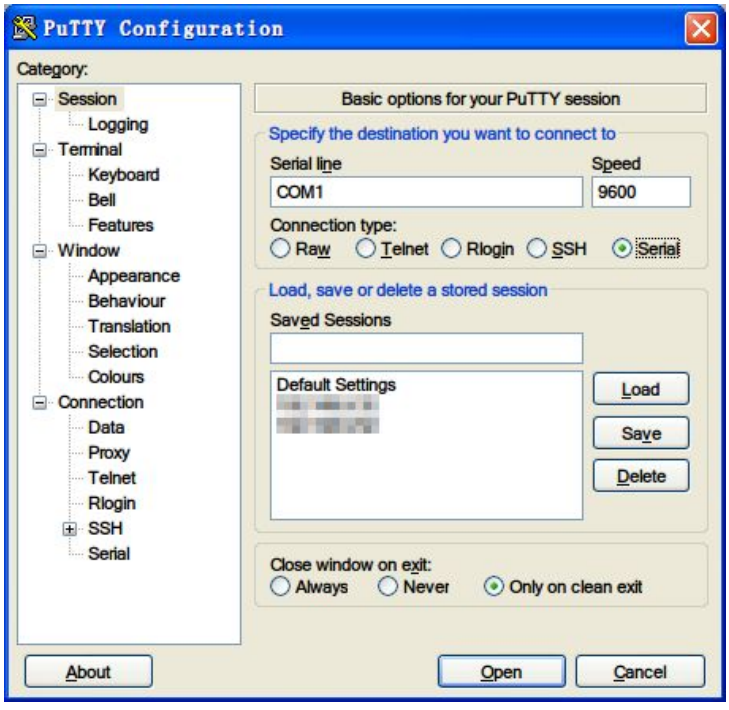
选择部署方案

参考 3、安装部署，选择适合自己网络拓扑结构的部署方式。

初始化设备

连接设备的 Console 口

1. 用 Console 线连接 PC 机和防火墙；
2. Console 线串口一端连接 PC 机串口，另一端连接设备的 Console 口；
3. 运行支持 COM 口通讯的软件（如 PuTTY、超级终端等）连接设备，连接状态选择“Serial”，波特率设置为 9600;



注意：

每台 PC 机的 COM 口设备编号可能不一样，请选择正确的 COM 口设备编号进行连接。

4. 设置好参数，点击【Open】按钮连接，输入用户名 conadmin，密码 conadmin 登陆系统，进入欢迎界面；

连接设备的 DSI 接口

使用网线将一台计算机直接连接至本设备的 DSI 接口，（请参考 2.1. 面板说明）将该计算机设置为“自动获得 IP 地址”，而不要设置静态 IP 地址。

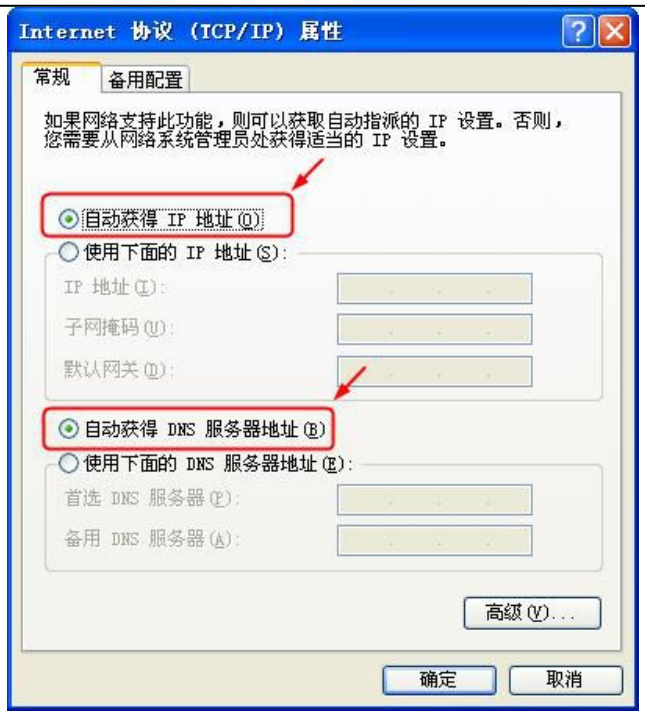
在 Microsoft Windows XP 下设置“自动获得 IP 地址”的方法如下：

（1）【开始】→【控制面板】→【网络连接】；

（2）在“本地连接”图标上点击右键，然后点击弹出的【属性】菜单。如图：

（3）在弹出的“本地连接 属性”对话框中选中“Internet 协议（TCP/IP）”，然后点击【属性】；

（4）在弹出的“Internet 协议（TCP/IP）属性”对话框中，选择“自动获得 IP 地址”和“自动获得 DNS 服务器地址”，然后点击【确定】；



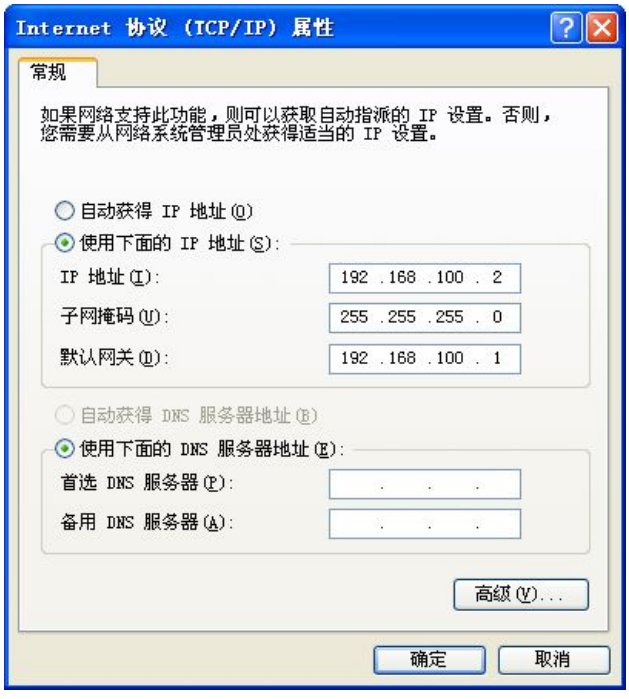
（5）等待并确认您的计算机通过 DHCP 获得了真实有效的 IP 地址，IP 地址应为 192.168.100.xx。

ⓘ提示：

如果通过步骤（4）“自动获得 IP 地址”无法自动获得有效的 IP 地址.

您也可以手工指定计算机的静态 IP 地址。

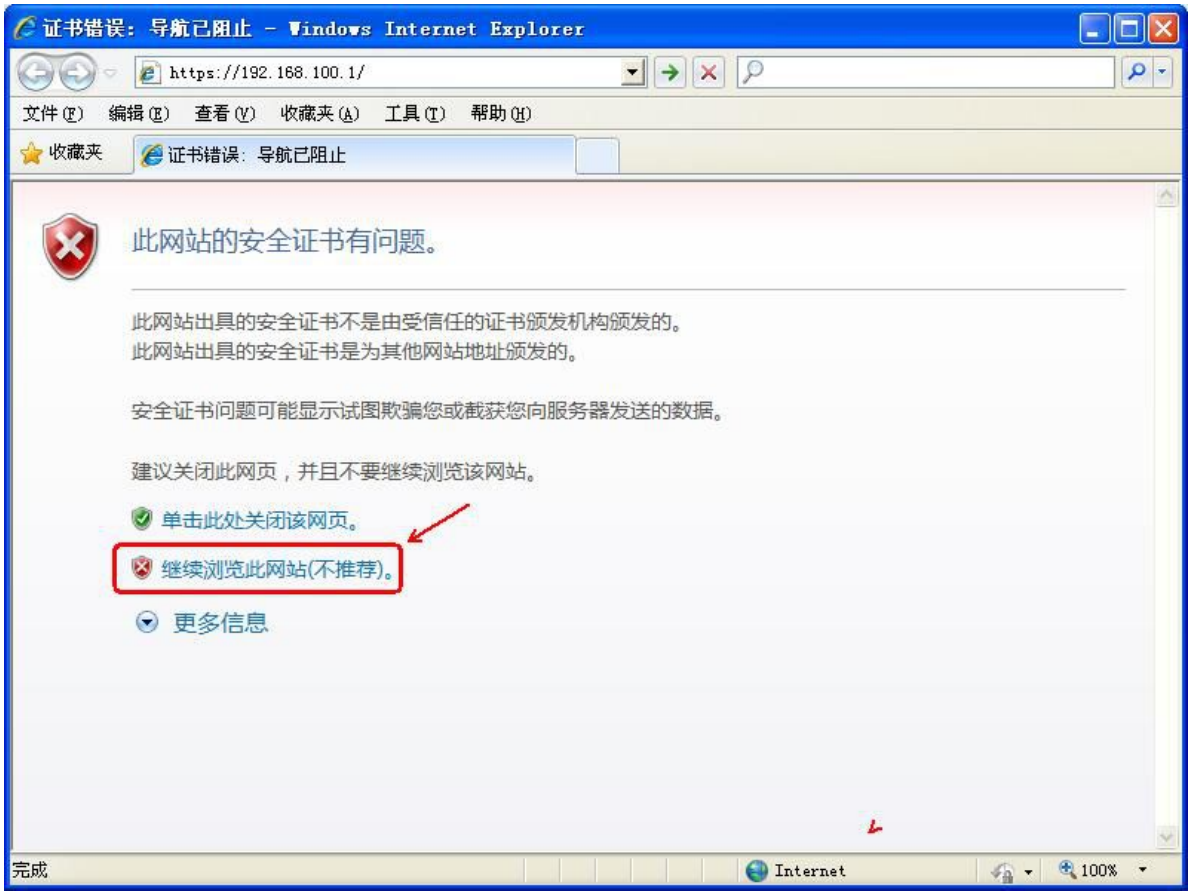
静态 IP 地址的设置参数如下：



配置 DMI 接口网络参数

假设您已经将计算机连接至本设备的 DSI 接口，并且通过 DSI 接口使您的计算机自动获得了 IP 地址。下面介绍配置 DMI 接口网络参数的操作方法：

（1）使用浏览器访问 https://192.168.100.1，浏览器可能会提示“此网站的安全证书有问题”，如图。



提示：

如果无法访问该网址，请检查计算机的防火墙设置，需要打开 443 端口才能访问此网址。

（2）点击“继续浏览此网站（不推荐）”，然后显示系统登录页面。如图。

（3）输入用户名和密码（设备初始用户名和密码请参看附录 A），点击【登录】按钮，进入“铱迅漏洞扫描系统”欢迎界面。

⚠注意：

如果登录失败，请检查是否为以下原因引起：

1) **用户名输入错误**
2) **密码输入错误**
3) **没区分大小写。**

如果某用户连续登录失败超过设定的次数（缺省为 3 次），则该用户将被锁定 15 分钟，15 分钟后该用户自动解锁。

建议使用 Firefox、Google Chrome、 Microsoft Internet Explorer 8.0 及以上版本的浏览器，屏幕分辨率最好设置为 1024×768 及以上。

（4）点击【网络设置】→【网络接口】，然后双击接口属性为“DMI”的网络接口进行配置（以下简称为 DMI 接口，即设备管理接口），具体参数请根据内部管理网络的实际情况设置，配置完成后需要在“静态路由”配置相对应的默认网关地址。

⚠注意：

请联系网络管理员，以便获取正确的网络设置参数。

提示：

如果网络配置失败（包括 IP 地址填写错误，网关、DNS 配置错误等），从而无法访问设置好的网络接口的 IP 地址，请重新配置或者执行产品复位。

提示：

如果 DMI 接口的 IP 地址无法访问，请检查：

1. 确认部署环境中是否有防火墙，该防火墙中是否针对该 IP 地址进行了一些访问控制的限制；（比如：设置了 MAC 地址绑定。）
2. 确认该 IP 地址是否已经被别的主机占用。

修改默认路由

例如：

1. 序号为 1 的记录为默认路由，双击该记录，弹出“静态路由-修改”对话框；

2. 选择“接口名称”：即对应的网络接口名称，可以修改默认路由所在的接口，比如从 ETH4 改到 ETH3；
3. 勾选“设置为默认路由”；
4. 填写“网关”，这里添加的网关必须与【网络接口】页面中该网络接口的网关一致。并且默认路由的网关不能为空；
5. 点击【保存】按钮，返回上一级页面；

注意：

系统只能有一条默认路由，可以修改默认路由，但不能添加多条默认路由。

5、快速使用指南

修改密码

系统管理员登录“铱迅漏洞扫描系统”后，点击左边菜单栏【配置】→【用户设置】，选择 webadmin 用户，点击【修改】，重新设置密码。密码长度应该大于或等于设定的长度，且至少包含数字、大小写字母等字符。

- 系统管理员可以修改所有安全管理员和用户的密码；
- 安全审计员可以修改安全审计员的密码；
- 每个用户都可以修改自己的密码。点击右上角“欢迎您：某用户”，系统弹出该用户的密码修改对话框，如下图所示。

⚠注意：

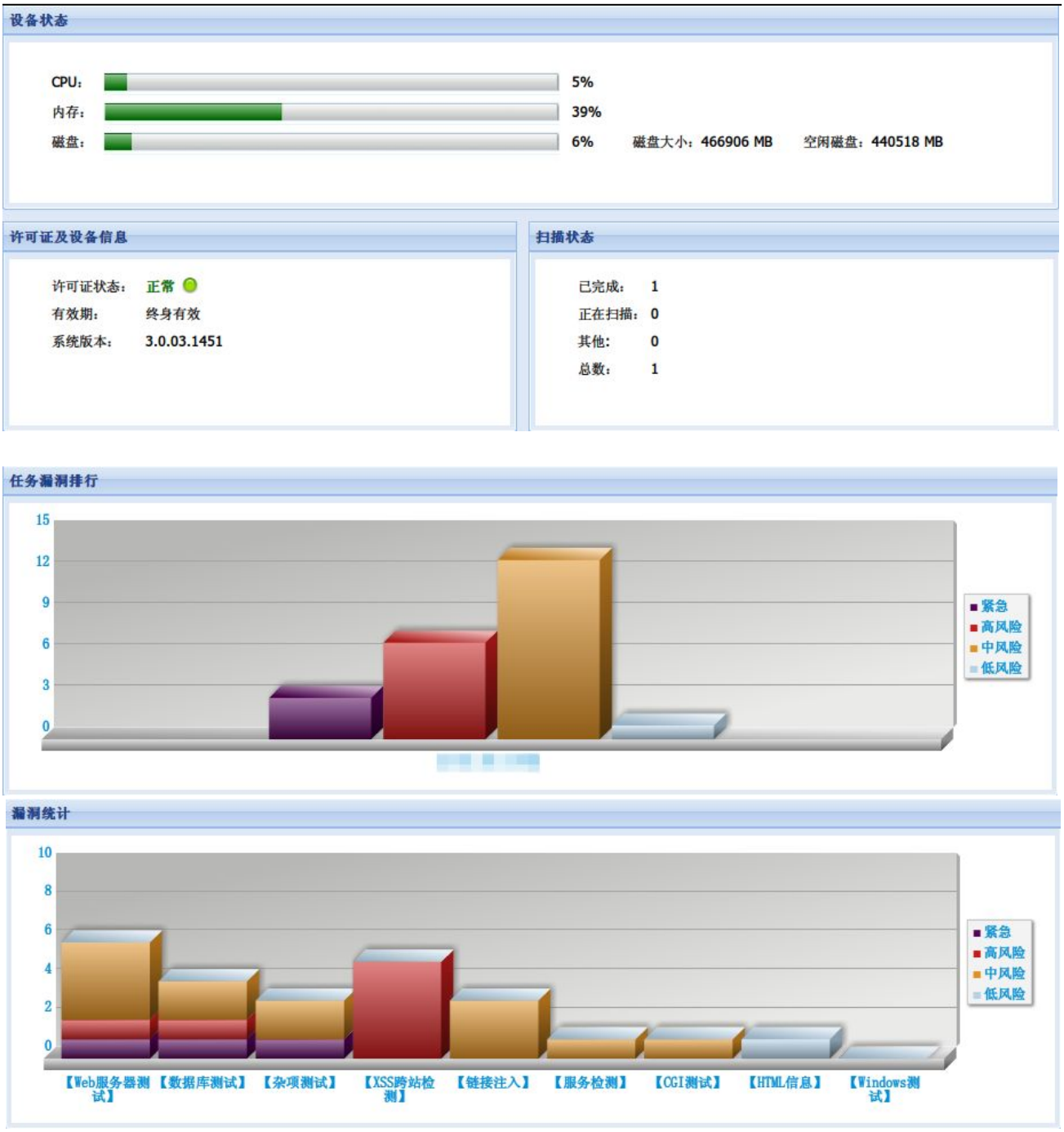
出于安全的考虑，强烈建议您在初次使用时修改管理员密码。

查看系统状态

点击左边菜单栏【状态】，在弹出的子菜单中分别点击【系统状态】、【设备信息】和【授权信息】 在显示出的页面中可以分别查看当前设备的系统状态（CPU、内存和磁盘的使用情况），设备信息， 授权信息等。具体详见下面各小节。

系统状态

用于显示设备的当前系统状态，如图。



- CPU： 显示当前设备的 CPU 使用情况。
- 内存： 显示当前设备的内存使用情况。
- 磁盘： 显示当前设备的磁盘使用情况。当磁盘空间不足时，会向管理员发送邮件提醒，并且会自动清理磁盘。如果需要手动清理磁盘，请参考 14.3 磁盘日志清理。
- 许可证及设备信息： 显示当前许可证状态，有效期以及系统版本。
- 扫描状态： 显示当前扫描任务的完成情况。
- 漏洞统计排行： 显示当前的扫描任务中网站漏洞数目排行。
- 漏洞统计： 显示扫描任务中存在的不同类型漏洞的数目。

提示：

本设备会尽可能多的使用内存以便提高性能，因此内存占用较大(超过 80%)是正常现象。

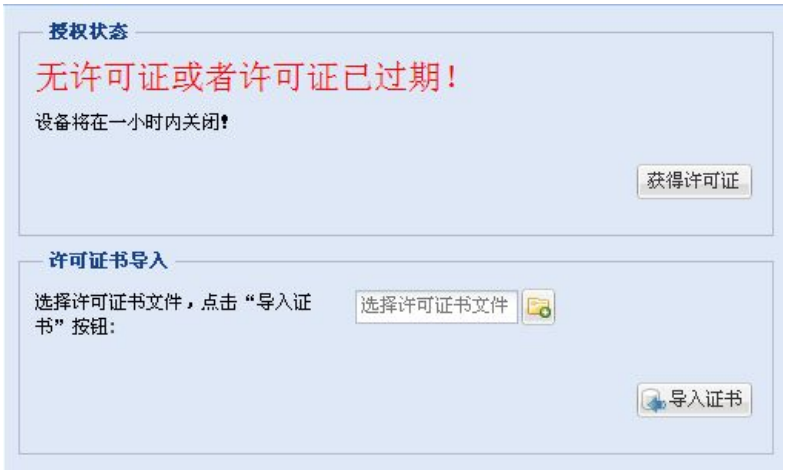
设备信息

用于显示本设备的硬件版本、固件版本、系统版本、产品型号和产品序列号。

授权信息

用于显示本设备的授权信息。每一台铱迅漏洞扫描系统都有唯一的许可证书，该许可证文件只能导入一次，重复导入相同证书无效。同时，许可证书不能在不同型号、同型号不同设备之间混用。

当设备没有许可证或者许可证已经过期的情况下，使用安全管理员账号登录时就会出现如下页面。



当本设备许可证是有效期授权类型的，使用安全管理员账号登录时，可以看到当前的许可证状态如下。

当本设备许可证是终身授权类型的，使用安全管理员账号登录时，可以看到当前许可证状态如下。

注意：

当设备没有许可证或者许可证已经过期，铱迅漏洞扫描系统将在一小时之内关机。如果遇到上述情况，请及时联系供货商或者铱迅信息以便获取有效许可证书。

实时流量

用于显示各个网络接口的实时流量信息。


刷新

网络接口	模式	速率	连接状态	收到的数据包	发送的数据包	收到的字节	发送的字节	收到的错误包	丢失接收的包	接收速率	发送速率
ETH0	自动	自动		0	0	0	0	0	0	0bps	0bps
ETH1	全双工	1000 Mbps		30086068	1981777	4.6 GB	401.97 MB	7	15548	0 bps	0 bps
ETH2	自动	自动		0	0	0	0	0	0	0bps	0bps
ETH3	自动	自动		0	0	0	0	0	0	0bps	0bps
ETH4	自动	自动		0	0	0	0	0	0	0bps	0bps
ETH5	自动	自动		0	0	0	0	0	0	0bps	0bps

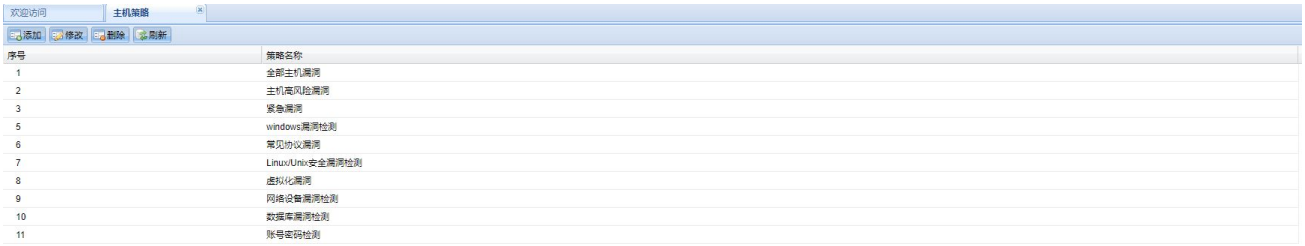
网络流量

该页面统计并显示网络接口的网络流量，可以按天或者按月以折线图的形式显示出来。

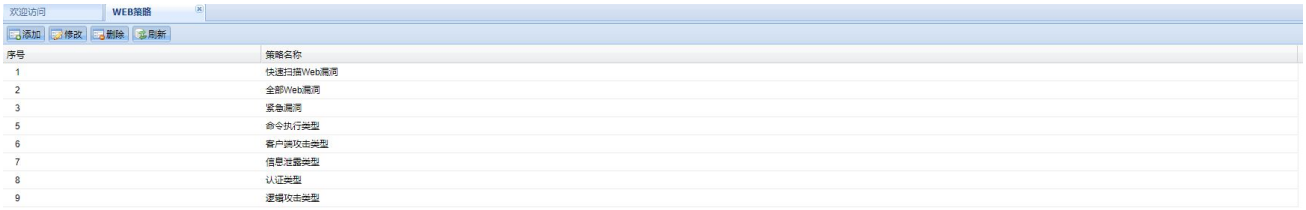
查看扫描策略管理

点击左边菜单栏【策略管理】，可以管理漏洞扫描的策略。

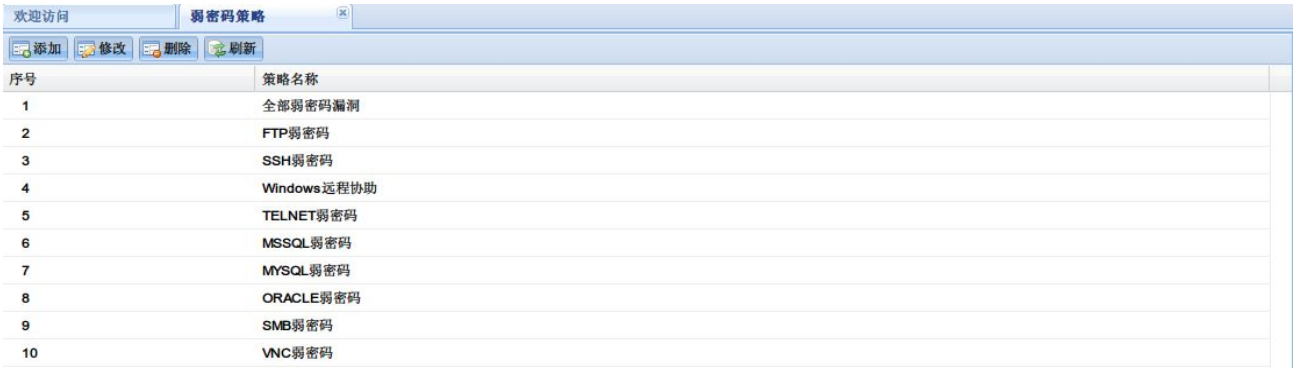
主机策略：管理主机漏洞扫描的策略。



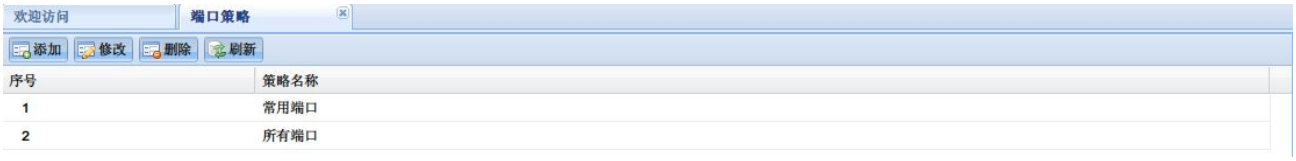
WEB 策略：管理 Web 漏洞扫描的策略。



弱密码策略：管理弱密码扫描的策略。



端口策略：管理端口扫描的策略。



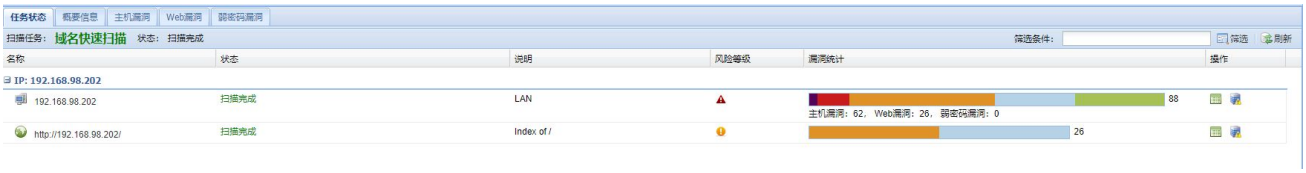
您可以添加或删除漏洞扫描的策略。详细操作请参考《铱迅漏洞扫描系统管理员手册》。

提示：

本设备默认扫描策略不可修改与删除，用户自行添加的扫描策略可修改删除！

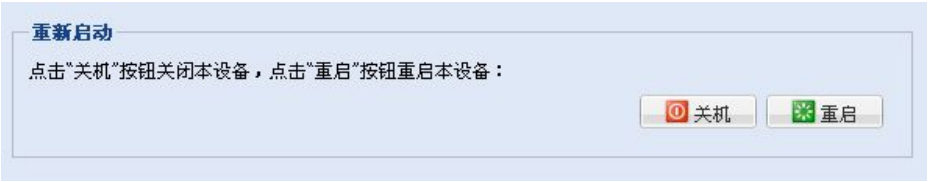
查看漏洞扫描任务及扫描详细信息

点击欢迎界面【漏洞扫描】，弹出【漏洞扫描】界面，选择一条任务，点击任务名，进入扫描详细信息，可查看扫描结果。



关机和重启

点击左边菜单栏【系统】→【重新启动】，在【重新启动】页面中可以选择“关机”和“重启”。



⚠注意：

请您尽量避免在本设备运行的时候直接切断电源。这样可能造成数据的丢失或影响设备的使用寿命。

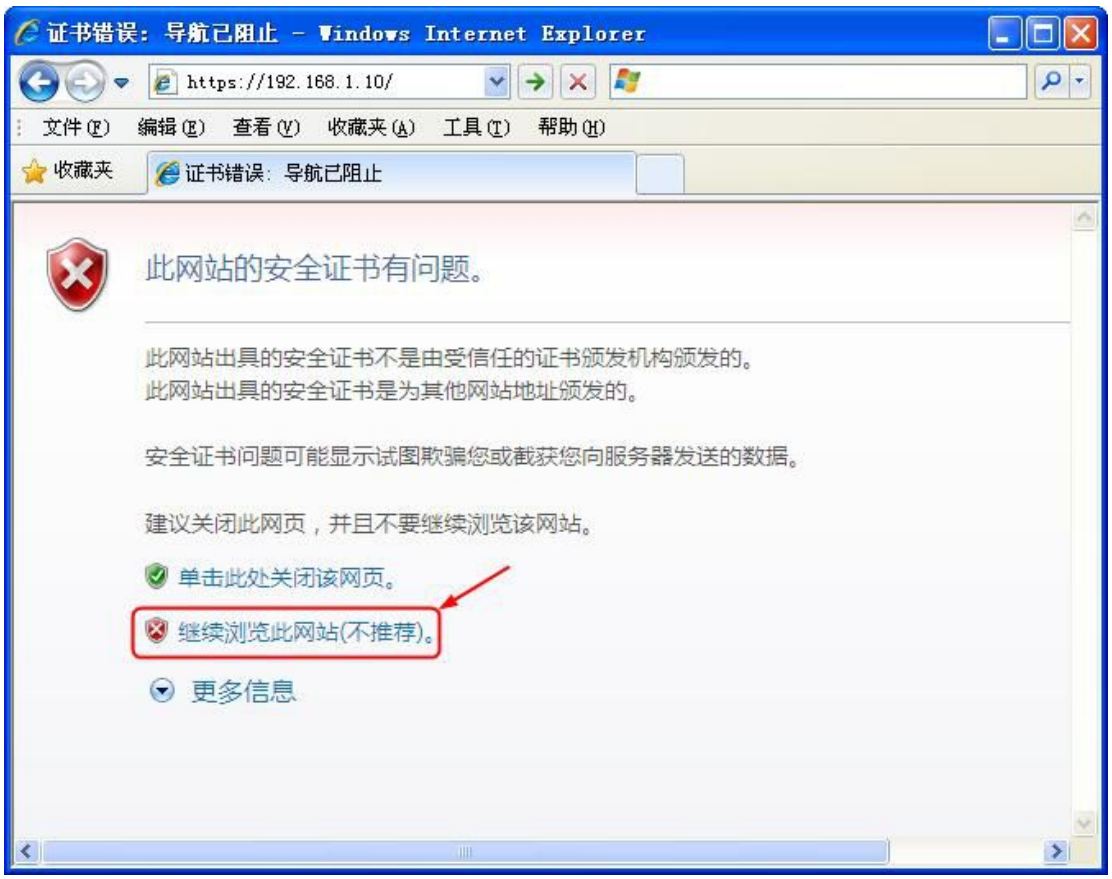
在您点击【关机】按钮，或者直接按下设备上的电源按钮后，请等待设备电源指示灯熄灭后再切断电源。设备安全关闭需要一定时间。

6、开始使用

登录

登录系统

在浏览器中输入您已经配置好的本设备 DMI 接口的访问地址(如:https://192.168.1.10)后按回车(Enter)键，浏览器可能会提示“此网站的安全证书有问题”，如图。



点击“继续浏览此网站（不推荐）”，然后显示系统登录界面，如图。输入正确的用户名和密码，点击【登录】按钮即可登录到本设备进行操作。

提示:

如果是首次安装并使用本设备，请先仔细阅读 4. 设备安装及初始化相关章节。

关于如何配置本设备 DMI 接口的 IP 地址，具体请参考 4. 设备安装及初始化的相关章节。

出厂的默认用户名和密码请参考附录 A。

提示:

为了获得最佳的页面浏览效果，建议您使用 Firefox、Google Chrome、Microsoft Internet Explorer 8.0 及以上版本的浏览器，推荐显示分辨率 1024×768 以上。

注意:

如果连续登录失败的次数超过设定值（缺省为 3 次），则该用户将被锁定 15 分钟。15 分钟内不允许该用户登录。

系统管理员登录

系统管理员为系统内置账号，可创建并管理安全管理员、普通用户的账号，除此之外无其它权限。系统管理员的所有操作行为都被记录到审计日志。内置的系统管理员账户 sysadmin 不可删除。

系统管理员可以使用内置的 sysadmin 账号登录界面，如下图所示。

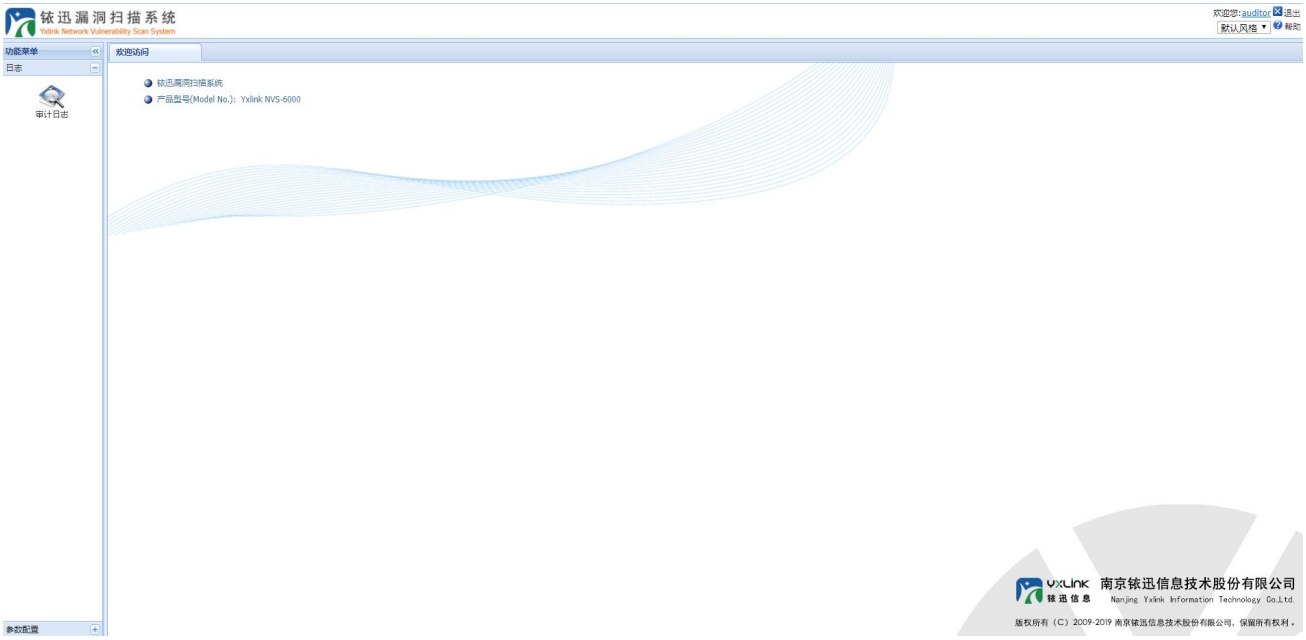
使用系统管理员账号登录成功后的欢迎界面，如下图所示。具体功能的介绍，请参见 12.14.1 用户设置（系统管理员适用）。

安全审计员登录

安全审计员只负责对系统管理员和安全管理员的操作日志进行查看和管理，还负责管理安全审计员类型的账号。

安全审计员可以使用内置的 auditor 账号登录界面，如下图所示。

使用安全审计员账号登录成功后的欢迎界面，如下图所示。



安全管理员登录

安全管理员负责产品安全策略制定、产品配置以及日常维护等管理，不能进行审计日志的查看和管理，不能创建系统管理员、普通用户、安全审计员账号。

安全管理员可以使用内置的 webadmin 账号登录界面，如下图所示。

使用安全管理员账号登录成功后的欢迎界面，如下图所示（具体功能的介绍，请参见后面的各个章节）

密码修改

当采用系统内置用户首次登录成功后，系统会强制要求修改用户的默认密码，对话框，如下：

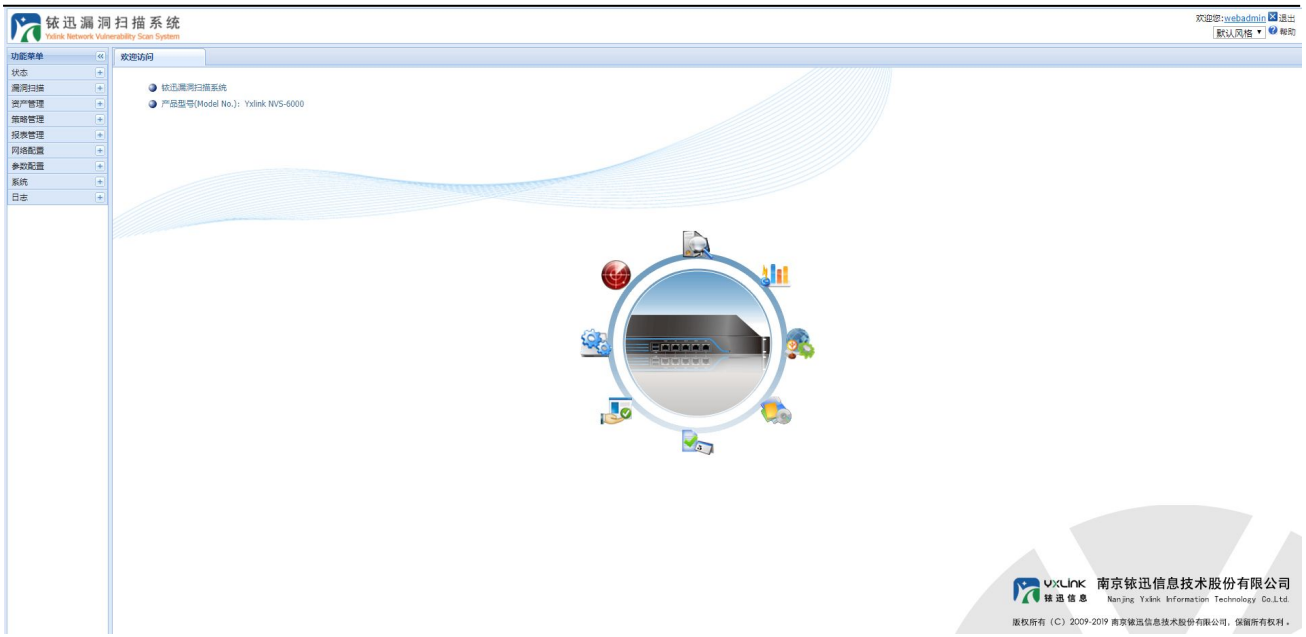
密码修改有三种方式：

- 系统管理员可以修改所有安全管理员和普通用户类型账号的密码；
- 安全审计员可以修改安全审计员类型账号的密码；
- 每个用户都可以修改自己的密码。

（点击右上角“欢迎您：某用户”，系统弹出该用户的密码修改对话框，如下图所）

欢迎界面

安全管理员在登录界面输入用户名和密码并通过验证后，将看到如图所示的欢迎界面。



整个界面划分为 5 个功能块，即左上侧的产品 Logo 图标，左侧的功能菜单列表，右上侧的登录信息，右侧中间的选项卡列表和右下侧的各种操作管理页面。

功能菜单列表：所有的操作管理页面都可以通过左侧的功能菜单点击进入。

1. 在【欢迎访问】页面中显示了本产品的设备型号和八个快捷方式，通过快捷方式，您可以快速地进入各种操作管理页面。
2. 当您打开不同的页面时，页面上方会显示出当前已经打开的所有选项卡。您可以点击选项卡以便快速地在各个打开页面之间来回切换。
3. 在欢迎页面的右上角，您可以点击【帮助】获取系统的帮助信息。
4. 当您选择【默认风格】或者其他风格时，整个管理界面的风格和配色方案会随之改变。
5. 您可以点击【退出】按钮，以便安全退出 Web 管理页面。
6. 点击产品 Logo 图标返回【欢迎访问】页面。

ⓘ提示：

按 F11 键可以让浏览器进入全屏浏览模式，提供更大的操作界面。

功能菜单

功能菜单包括以下主菜单，每个主菜单下面又有若干子菜单。

当您点击主菜单后，会弹出其下的子菜单。各个菜单的主要功能如下：

【状态】主菜单：

- 【系统状态】：查看本设备的当前状态。
- 【设备信息】：查看本设备的型号、固件版本等信息。
- 【授权信息】：查看本设备的许可证状态，以及许可证书的导入。

- 【实时流量】：查看本设备所有网络接口的实时状态，以及收发数据包、速率等。
- 【网络流量】：按天或者按月显示本设备的网络流量统计图，以便查看设备发出的数据包的状态。

【漏洞扫描】主菜单：

- 【漏洞扫描】：查看和管理进行漏洞扫描的网站，并且可查看该任务的扫描进度、扫描的漏洞数。

【策略管理】主菜单：

- 【主机策略】：管理主机漏洞扫描的策略。
- 【WEB 策略】：管理 WEB 漏洞扫描的策略。
- 【弱密码策略】：管理弱密码扫描的策略，支持 FTP、MYSQL、MSSQL、ORACLE、SSH 等弱密码扫描。
- 【端口策略】：管理主机端口扫描的策略。

【报表】主菜单：

- 【报表管理】：对生成的报表进行导出、筛选等管理。
- 【快速报表】：提供即时的生成系统报表的功能。
- 【条件报表】：可以提供条件选择生成报表的功能。

【网络配置】主菜单：

- 【网络接口】：查看和设置本设备的所有网络接口。
- 【静态路由】：配置本设备的静态路由。
- 【DNS 设置】：设置本设备的 DNS 服务器。
- 【接口管理】：对设备的 DSI，DMI 接口进行设置。
- 【VPN 设置】：设置 VPN。
- 【OpenVPN 设置】：设置 OpenVPN
- 【Socks 代理】：设置 Socks 代理。
- 【网卡限速】：限制网络接口的带宽。

【参数配置】主菜单：

- 【基本参数设置】：设置远程文件包含 URL 以及域名检查端口。
- 【通知设置】：设置邮件通知的管理员邮箱，当设备磁盘空间不足时，将自动发送邮件通知管理员进行磁盘清理工作。
- 【syslog】：设置 syslog 服务器的 IP 与端口，用于将信息同步到服务器。
- 【API 设置】：设置 API 配置，用户创建扫描任务、导出报表、下载扫描任务结果。
- 【FTP 字典】：添加 FTP 字典内容，用于弱密码扫描。
- 【MYSQL 字典】：添加 MYSQL 字典内容，用于弱密码扫描。
- 【MSSQL 字典】：添加 MSSQL 字典内容，用于弱密码扫描。
- 【ORACLE 字典】：添加 ORACLE 字典内容，用于弱密码扫描。
- 【TELNET 字典】：添加 TELNET 字典内容，用于弱密码扫描。

- 【远程协助字典】：添加远程协助字典内容，用于弱密码扫描。
- 【SMB 字典】：添加 SMB 字典内容，用于弱密码扫描。
- 【SSH 字典】：添加 SSH 字典内容，用于弱密码扫描。
- 【VNC 字典】：添加 VNC 字典内容，用于弱密码扫描。
- 【网页木马文件名字典】：添加网页木马文件名字典内容，用于 Web 漏洞扫描。
- 【WEB 弱密码字典】：添加 WEB 弱密码字典内容，用于 Web 漏洞扫描。
- 【WEB 页面关键字字典】：添加 WEB 页面关键字字典内容，用于 Web 漏洞扫描。
- 【Tomcat 管理后台弱密码】：添加 Tomcat 管理后台弱密码内容，用于 Web 漏洞扫描。

【系统】主菜单：

- 【固件升级】：升级本设备中的软件和安全补丁。
- 【系统配置】：设置系统时间等。
- 【网络工具】：提供常用的 ping、route、arp、traceroute 和 nslookup 等网络诊断工具。
- 【重新启动】：关闭或重启本设备。

【日志】主菜单：

- 【系统日志】：查看系统日志，记录了系统相关的事件信息。
- 【磁盘日志清理】：对过期日志进行备份或者删除，清理磁盘空间，以便于系统良好的运行。

通用菜单、按钮介绍

保存和应用功能

如图，在许多页面中都有【保存】和【应用】按钮。

【保存】按钮的含义是保存当前的设置更改但并不立即生效。

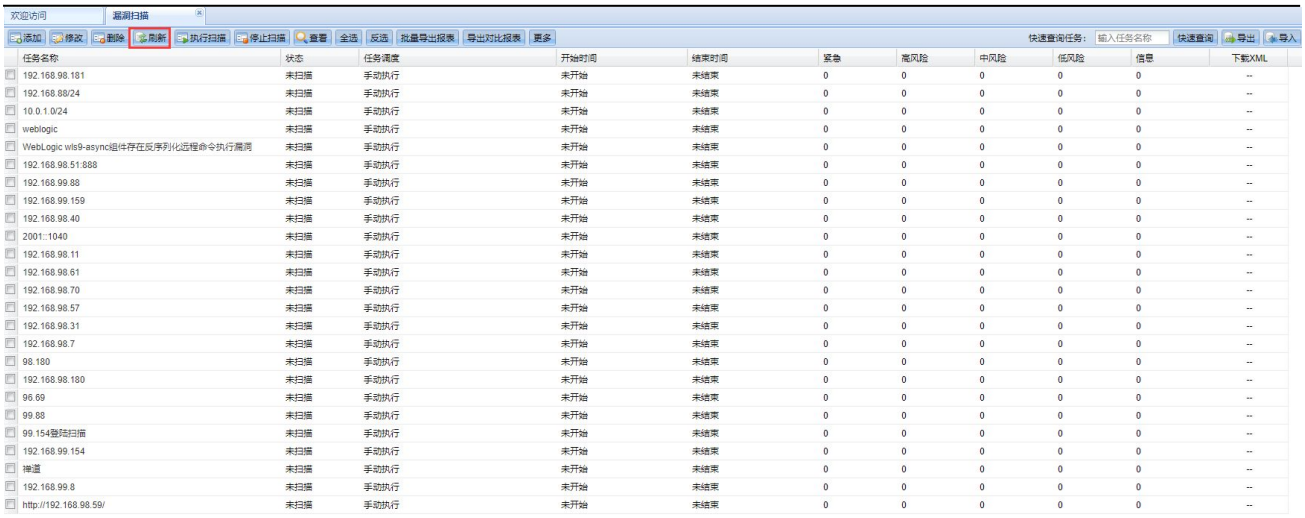
【应用】按钮的含义是保存当前的设置更改并立即生效。

注意：

建议在每次设置更改后点击【保存】按钮。将所有设置全部配置完成以后，再点击【应用】按钮让所有设置更改生效。频繁点击【应用】按钮会降低系统的工作效率。

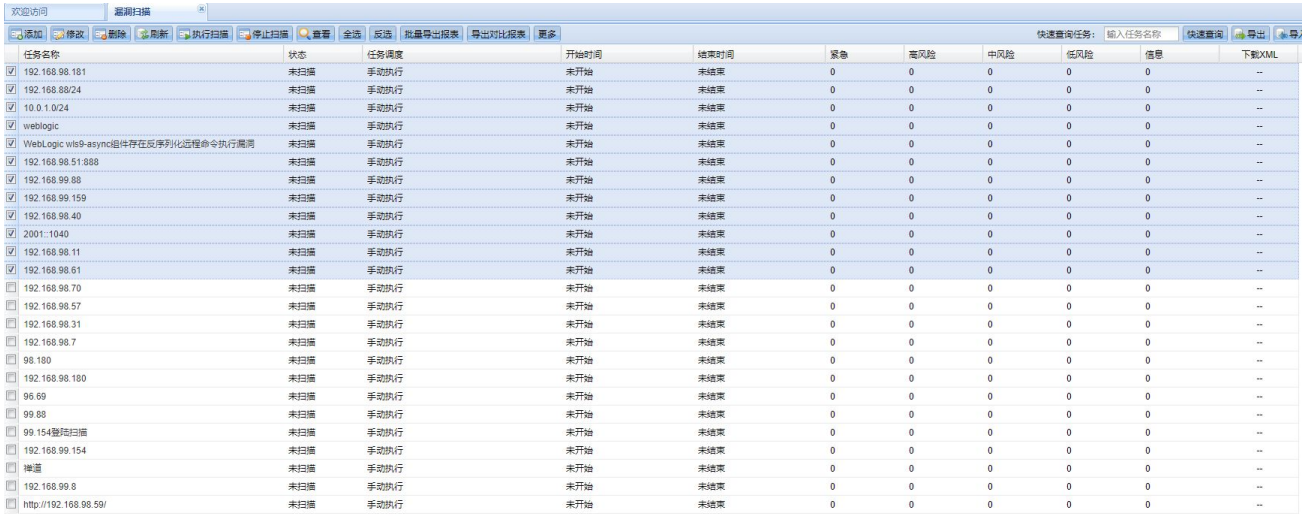
刷新功能

如图，【刷新】按钮的含义是从设备数据库中获取最新的数据到用户界面。当您觉得当前 Web 页面显示的信息已经过期的情况下可使用此按钮强制刷新。



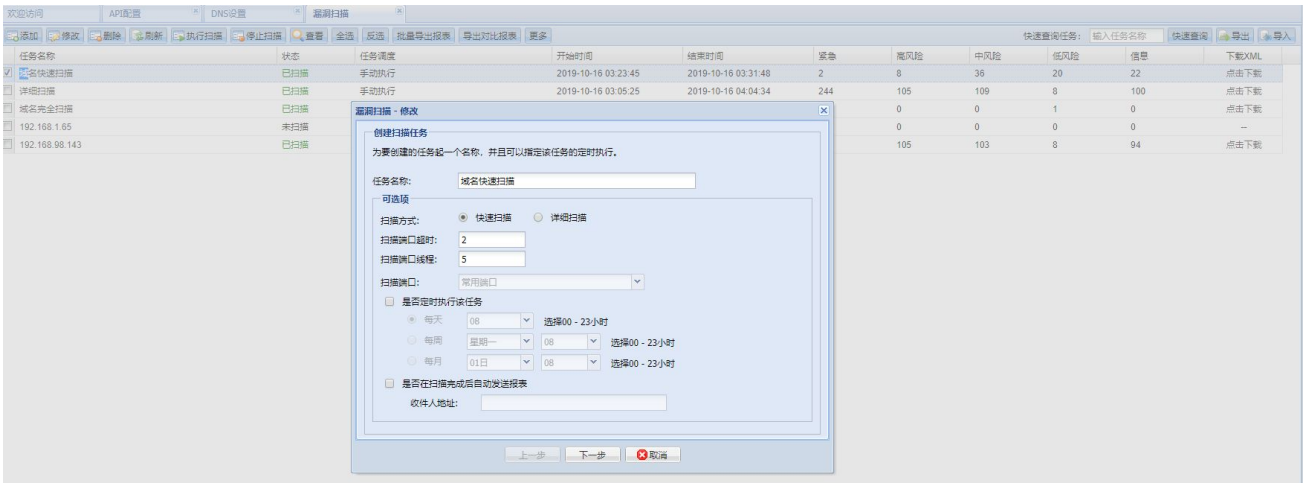
多选功能

如图，在大多数支持列表操作的页面中，您都可以通过按住 Ctrl 键点击以选择多条记录，或者通过按住 Shift 键选择开始记录和结尾记录以便选择一个记录范围。您也可以两种方法配合使用。



双击功能

在大多数支持列表操作的页面中，您可以通过双击某条记录，以便快速地进行相应的操作。如图，例如您在漏洞扫描界面双击一条记录时，系统会自动打开该条任务的编辑页面。



翻页功能

如图，在以列表显示的页面中，您可以通过左下角的翻页按钮来翻页：

表示跳到首页

表示上一页

表示下一页

表示跳到末页

漏洞扫描的状态

如图，在"漏洞扫描"和"扫描详细信息"的页面中，您可以看到扫描的状态，共分为 5 种：未扫描、正在扫描、暂停扫描、已扫描、等待。

：该状态为正在扫描。

：该状态为等待（比如：默认最大执行任务数为 5，需要执行的任务数超过最大执行任务数时，剩余任务的扫描状态为等待；如果有一条任务扫描完，状态为等待的任务将被自动执行）。

漏洞风险等级

本设备中漏洞风险等级分为 5 类：紧急、高风险、中风险、低风险、信息。

：表示紧急。

：表示高风险。

：表示中风险。

：表示低风险。

：表示信息。

扫描详细信息中的图标说明

：表示扫描的主机。

：表示扫描的域名。

：点击可以查看扫描的主机信息或域名信息。

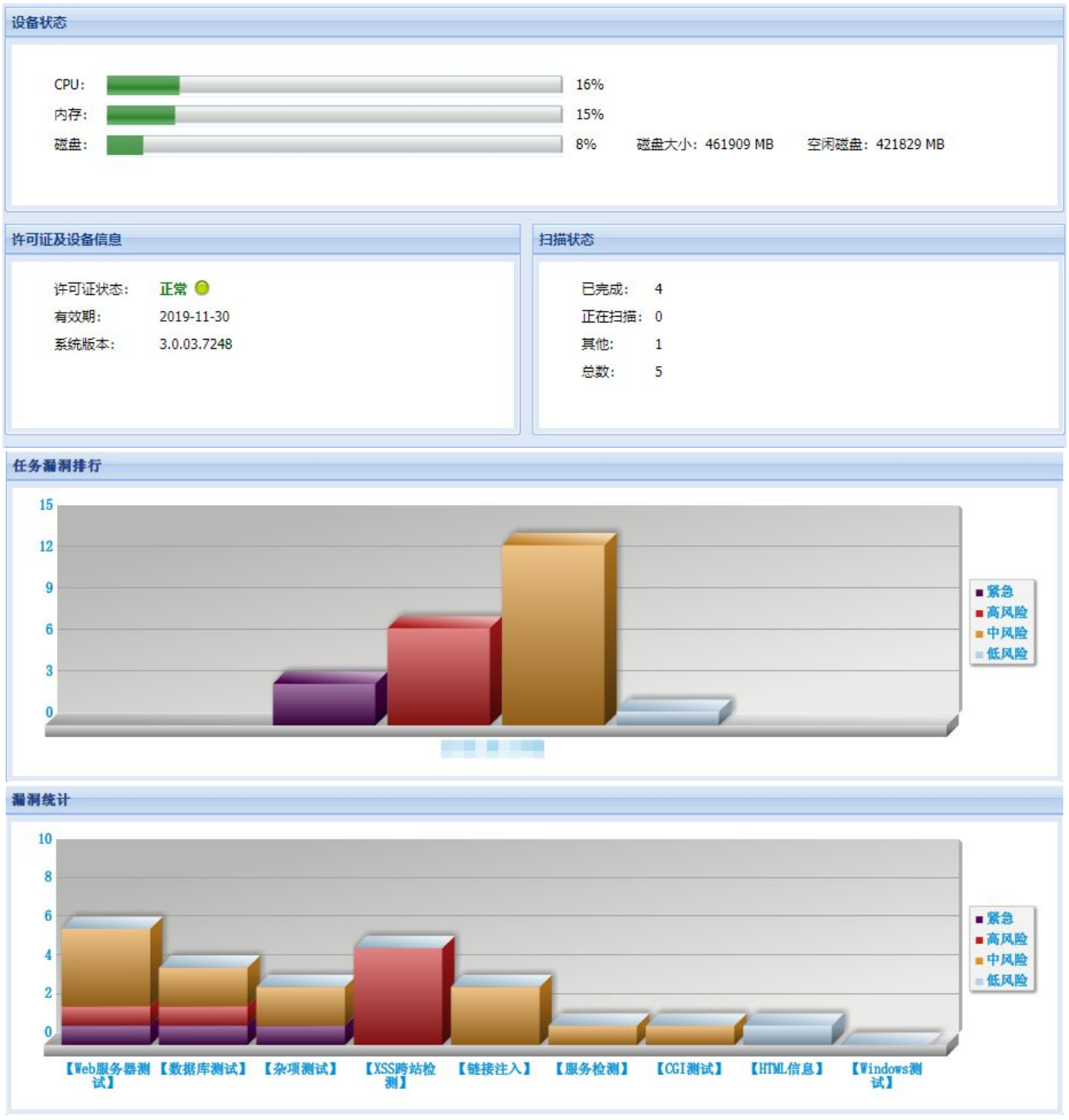
：点击可以查看扫描的主机漏洞或 Web 漏洞。

7、状态

用于查看当前设备的基本状态信息，包括四个部分：系统状态、实时流量、设备信息、授权信息和网络流量。

系统状态

用于显示设备的当前系统状态，如图。



- CPU： 显示当前设备的 CPU 使用情况。

- 内存： 显示当前设备的内存使用情况。
- 磁盘： 显示当前设备的磁盘使用情况。当磁盘空间不足时，会向管理员发送邮件提醒，并且会自动清理磁盘。如果需要手动清理磁盘，请参考 14.3 磁盘日志清理。
- 许可证及设备信息：显示当前许可证状态，有效期以及系统版本。
- 扫描状态：显示当前扫描任务的完成情况。
- 漏洞统计排行：显示当前的扫描任务中网站漏洞数目排行。
- 漏洞统计：显示扫描任务中存在的不同类型漏洞的数目。

提示：

本设备会尽可能多的使用内存以便提高性能，因此内存占用较大（超过 80%）是正常现象。

设备信息

用于显示本设备的硬件版本、固件版本、系统版本、产品型号和产品序列号。

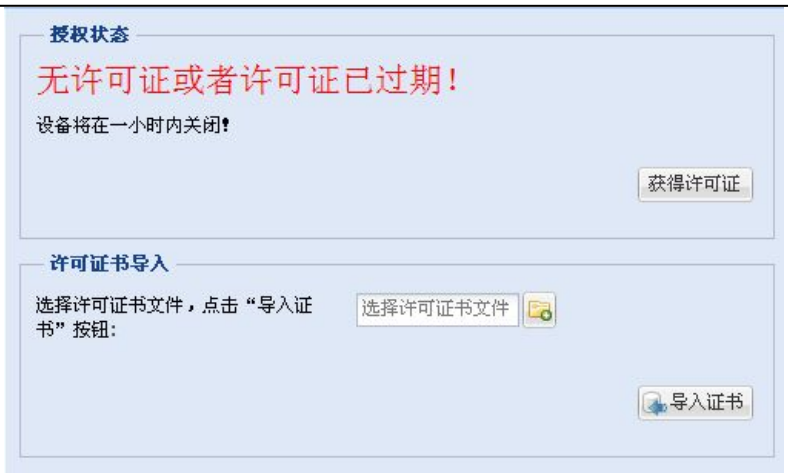
注意：

请记录下您使用产品的“产品序列号”等重要信息，以便在设备升级或出现故障的情况下，快速向铱迅客服人员请求帮助。

授权信息

用于显示本设备的授权信息。每一台铱迅漏洞扫描系统都有唯一的许可证书，该许可证文件只能导入一次，重复导入相同证书无效。同时，许可证书不能在不同型号、同型号不同设备之间混用。

当设备没有许可证或者许可证已经过期的情况下，使用安全管理员账号登录时会显示如下页面。



当本设备许可证是有效期授权类型的，使用安全管理员账号登录时，可以看到当前的许可证状态如下。

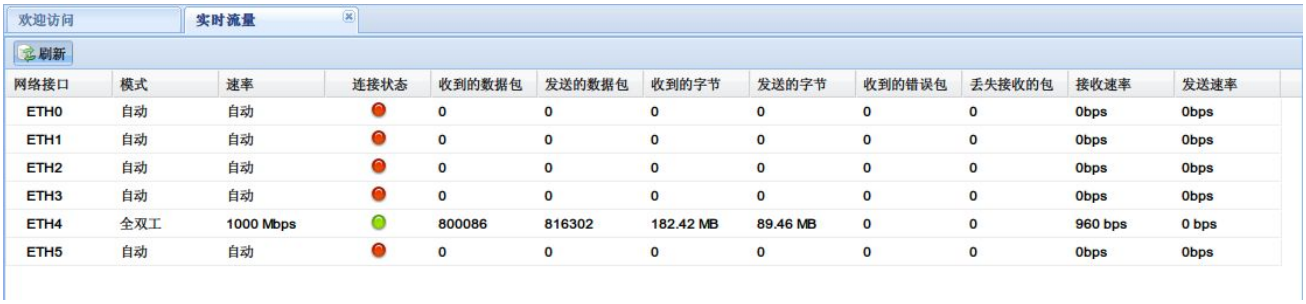
当本设备许可证是终身授权类型的，使用安全管理员账号登录时，可以看到当前许可证状态如下。

注意：

当设备没有许可证或者许可证已经过期时，铱迅漏洞扫描系统将在一小时之内关机。如果遇到上述情况，请及时联系供货商或者铱迅信息以便获取有效许可证书。

实时流量

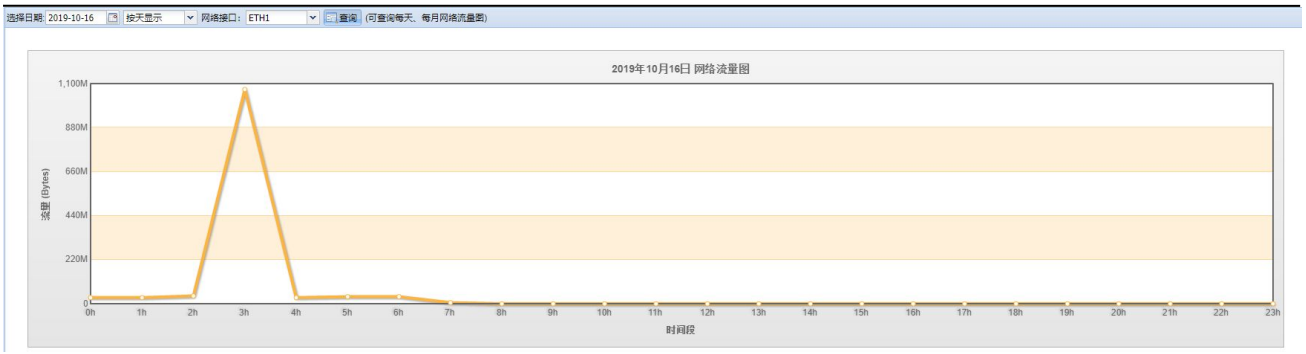
用于显示各个网络接口的实时流量信息。



网络接口	模式	速率	连接状态	收到的数据包	发送的数据包	收到的字节	发送的字节	收到的错误包	丢失接收的包	接收速率	发送速率
ETH0	自动	自动		0	0	0	0	0	0	0bps	0bps
ETH1	自动	自动		0	0	0	0	0	0	0bps	0bps
ETH2	自动	自动		0	0	0	0	0	0	0bps	0bps
ETH3	自动	自动		0	0	0	0	0	0	0bps	0bps
ETH4	全双工	1000 Mbps		800086	816302	182.42 MB	89.46 MB	0	0	960 bps	0 bps
ETH5	自动	自动		0	0	0	0	0	0	0bps	0bps

网络流量

该页面统计并显示网络接口的网络流量，可以按天或者按月以折线图的形式显示出来。

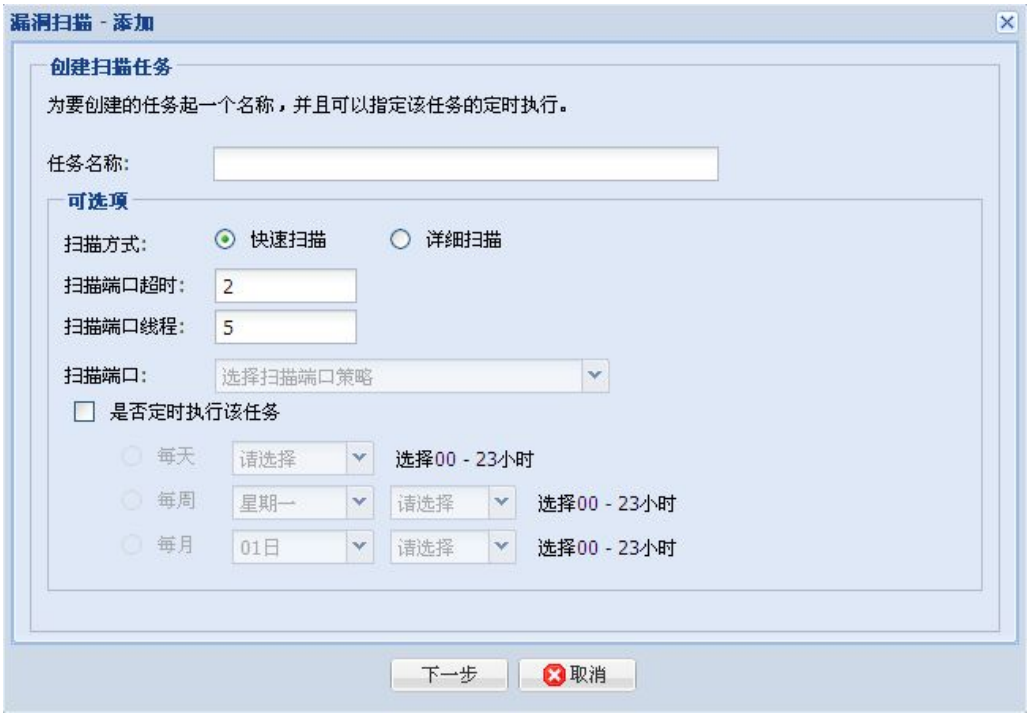

选择日期: 2019-10-16
按天显示
网络接口: ETH1
查询
(可查询每天、每月网络流量图)
2019年10月16日 网络流量图
1,100M
880M
660M
440M
220M
0
流量 (Bytes)
0h
1h
2h
3h
4h
5h
6h
7h
8h
9h
10h
11h
12h
13h
14h
15h
16h
17h
18h
19h
20h
21h
22h
23h
时间段

8、漏洞扫描

漏洞扫描

对需要扫描的 IP 地址或者网站执行添加、修改、删除、开始扫描以及停止扫描任务等操作。

- 添加漏洞扫描的网站：点击【添加】按钮，弹出“漏洞扫描-添加”对话框，输入扫描任务名称，还可以根据需要，选择勾选“扫描方式”与“是否定时执行该任务”，设置完成，点击【下一步】，继续添加。



扫描方式：

支持目标系统信息收集，探测目标系统使用的操作系统以及端口信息等。

- 快速扫描：只扫描主机的基本信息。
- 详细扫描：扫描主机的基本信息、可能的操作系统、端口等详细信息。
- 扫描端口超时：设置扫描端口的超时时间。
- 扫描端口线程：设置扫描端口的线程数。

- 扫描端口：设置所需要扫描的端口，具体可在【端口策略】中进行设置。
- 是否定时执行该任务：设置该任务的任务调度，手动执行与自动执行；可设置每天、每周、每月定时扫描该任务。

⚠ 注意：

如果当前扫描任务数为最大执行任务数时，定时任务不能自动执行，系统日志中会有相关提示！

为扫描任务设置相应的配置选项，包括主机漏洞扫描：

- 是否开启：设置是否开启主机漏洞扫描。
- 允许 DDOS 扫描：设置是否使用 DDOS 扫描。
- 扫描线程：设置主机漏洞扫描的线程数。
- 最大执行脚本数：设置漏扫的最大执行脚本数。
- 扫描策略 ：设置对主机漏洞扫描的策略。

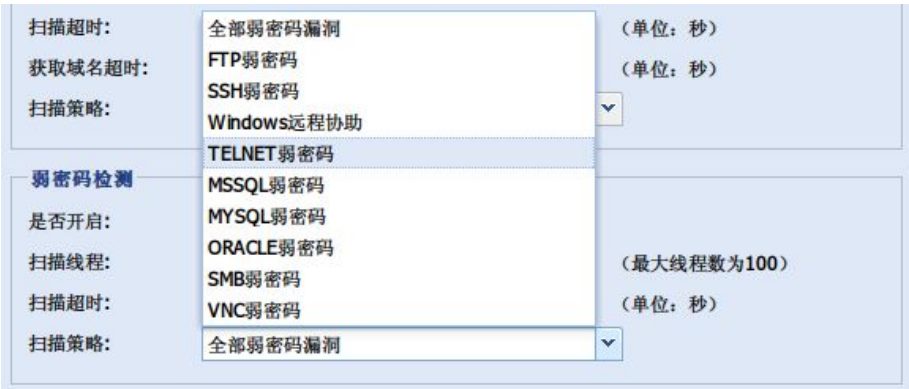
Web 漏洞扫描：

- 是否开启：设置是否开启 Web 漏洞扫描，以及设置是否开启域名反查（通过 IP 反查出该 IP 下的域名）。

- 扫描线程：设置系统最大执行的线程数。
- 爬虫最大地址数：设置域名抓取 URL 的最大数目。
- 扫描超时：设置扫描 Web 漏洞的超时时间。
- 获取域名超时：设置获取域名的超时时间。
- 通信异常请求次数：设置访问域名出现通信异常后尝试请求的次数。
- 通信异常请求间隔：设置访问域名出现通信异常后尝试请求的间隔时间。
- 扫描策略：设置对 Web 漏洞扫描的策略。

弱密码检测：

- 是否开启：设置是否开启弱密码检测。
- 扫描线程：设置最大执行的线程数。
- 扫描超时：设置弱密码扫描的超时时间。
- 扫描策略：设置弱密码检测的策略。

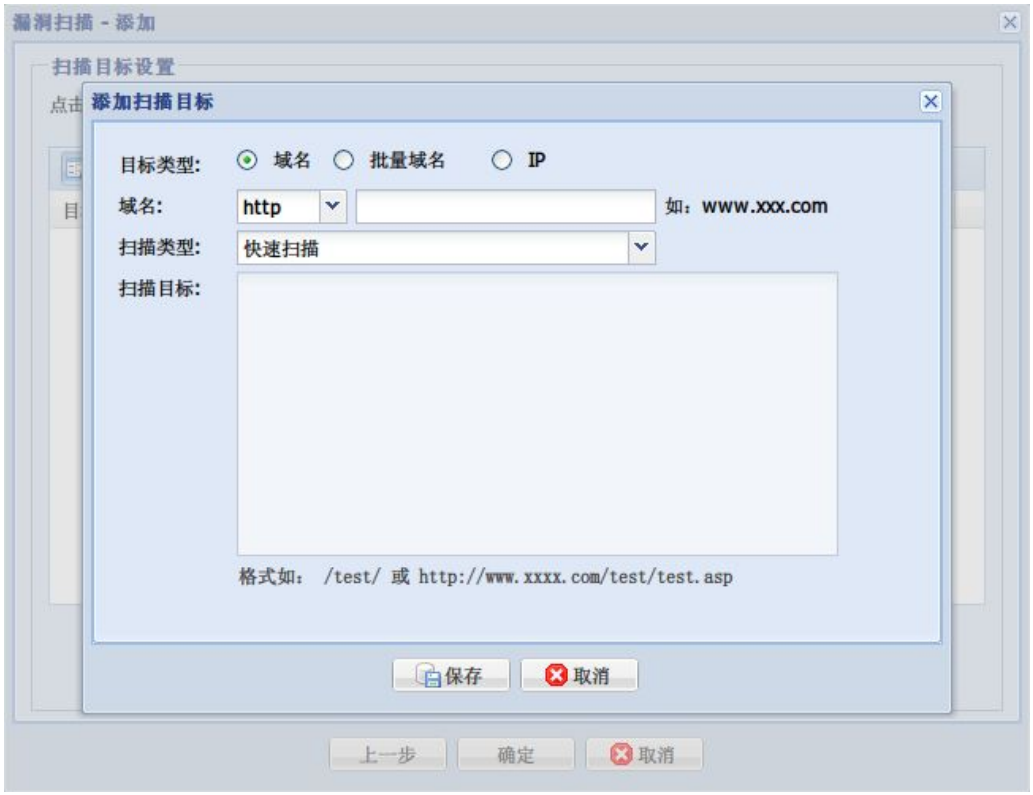


注意：

当线程数调到很大时，会缩短扫描时间，但是可能影响到扫描结果的准确性。

设置完成后，进入下一步“添加扫描目标”对话框。

扫描目标的设置：



可以添加“域名”、“IP”、“IP 段”、“批量域名”、“批量 IP 段”作为扫描任务目标，添加完成后点击【确定】，就可以完成对扫描任务的添加。

扫描类型说明：

1. “快速扫描”：只扫描当前域名的主机漏洞及 Web 漏洞。
2. “完全扫描”：扫描当前域名以及该域名下的二级域名的主机漏洞及 Web 漏洞。
3. “只扫描当前目录和子目录”：扫描当前域名目录和子目录的主机漏洞及 Web 漏洞。“扫描目标”填写该域名下的目录，例如格式为：/test/。
4. “只扫描任务目标 URL”：扫描当前域名下目标 URL 主机漏洞及 Web 漏洞。"扫描目标”填写该域名下的 URL，例如格式为：http://www.xxxx.com/test/test.asp。
5. “登录扫描”：通过“登录 URL”和“导入 cookie”（用户名和密码登录时获取的 cookie）网站后台进行扫描。获取 cookie 时需用到网络配置-HTTP 代理。

提示：

扫描任务添加完成后，系统会提示是否“任务添加成功，是否立即执行扫描”，当点击【是】按钮时，页面会自动跳转到“扫描详细信息”页面。

- 修改漏洞扫描的任务：选择需要修改的记录，点击【修改】按钮，进入“漏洞扫描-修改”窗口。（双击任务同样可以修改漏洞扫描任务）
- 删除漏洞扫描的任务：选择需要删除的记录，点击【删除】按钮，在弹出的确认对话框中点击【是】按钮，删除成功。
- 【执行扫描】：选中需要开始扫描的记录，点击【执行扫描】按钮，如果该任务从未被扫描过，则会弹出下面的提示，选择是，就可以开始扫描任务。

如果扫描任务处于暂停扫描的状态，点击【执行扫描】按钮，则会弹出下面的提示，可以根据自己的需要，选择“继续扫描”或“重新扫描”。

- 【停止扫描】：选中需要开始扫描的记录，点击【停止扫描】按钮，可以将正在扫描的任务暂停。
- 【查看】：选中需要开始扫描的记录，点击【查看】按钮，弹出扫描详细信息窗口，显示该任务的扫描信息。
- 导出扫描结果：选中需要开始扫描的记录，点击【导出扫描结果】按钮，可以将该扫描结果导出，扩展名为 bak 格式。
- 导入扫描结果：选中需要开始扫描的记录，点击【导入扫描结果】按钮，弹出导入扫描结果窗口，选择对应的文件可以将文件导入。

注意：

如果扫描详细信息页面中的内容一直为空，可能是 DNS 或者网络配置不正确。请检查“网络配置”-“静态路由”与“网络配置”-“DNS 设置”是否配置正确，确认配置正确后再次【执行扫描】即可。

提示：

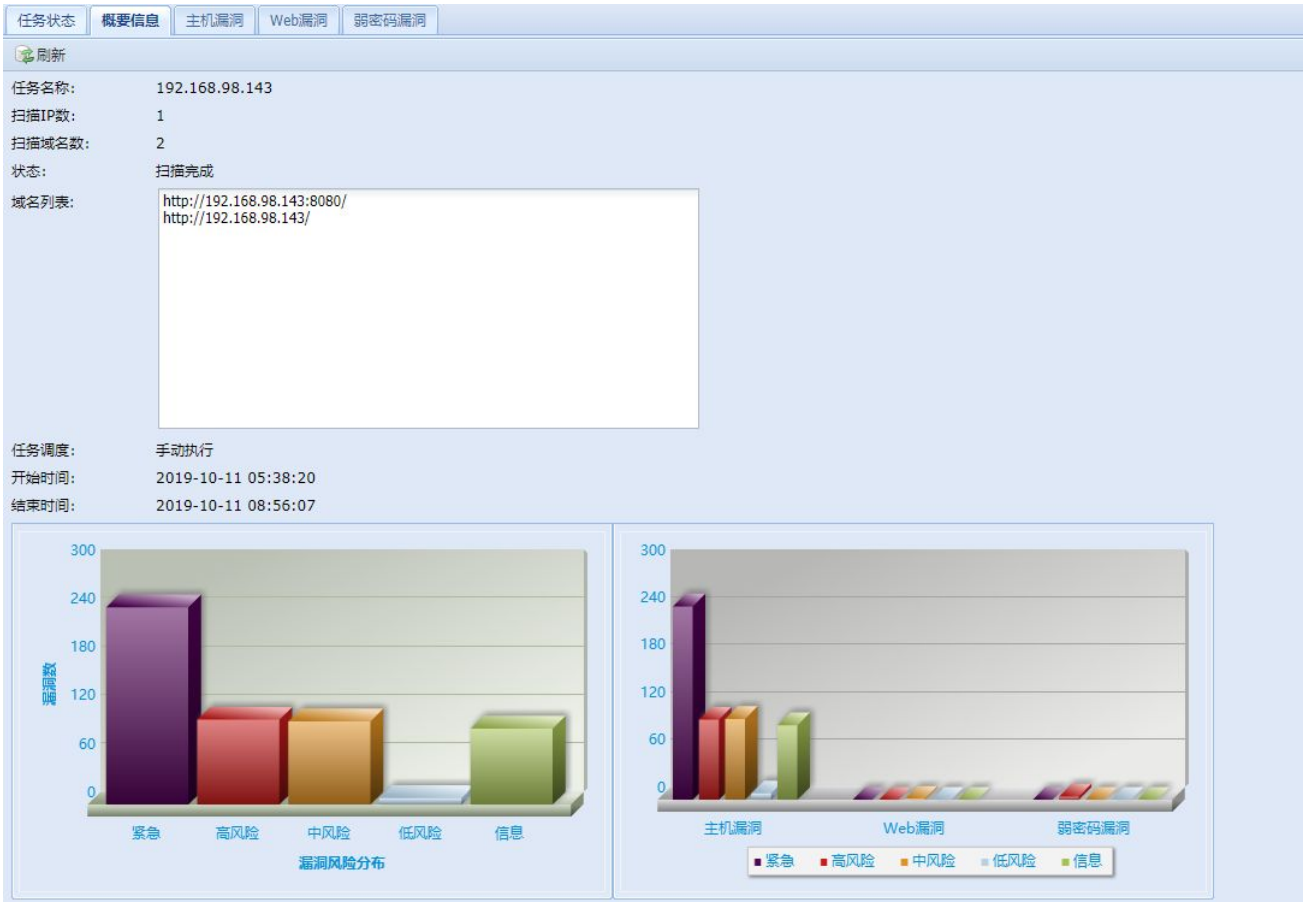
可以对相同状态的任务进行批量操作（例如：执行扫描、停止扫描）。

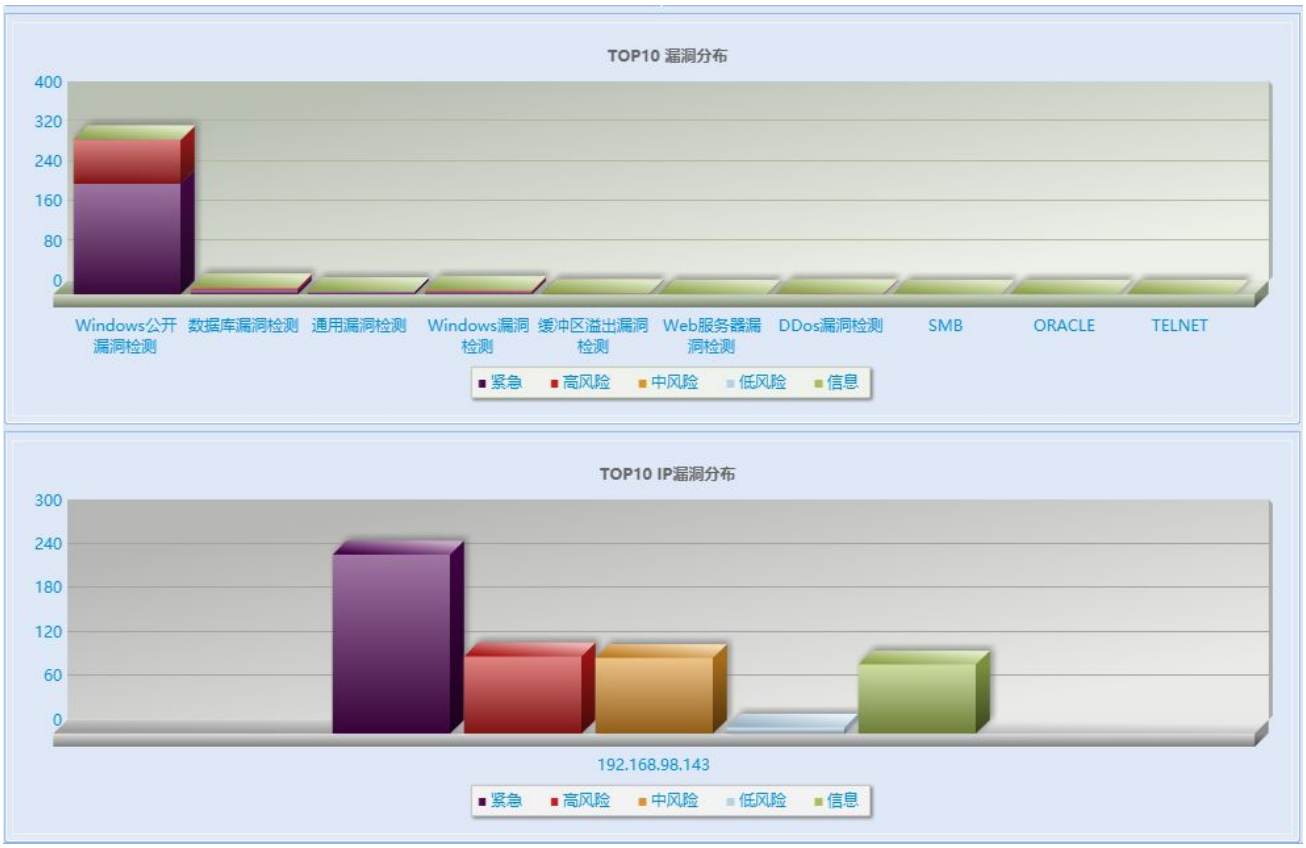
扫描详细信息

在“漏洞扫描”页面中，点击一个任务名即可进入【扫描详细信息】页面。

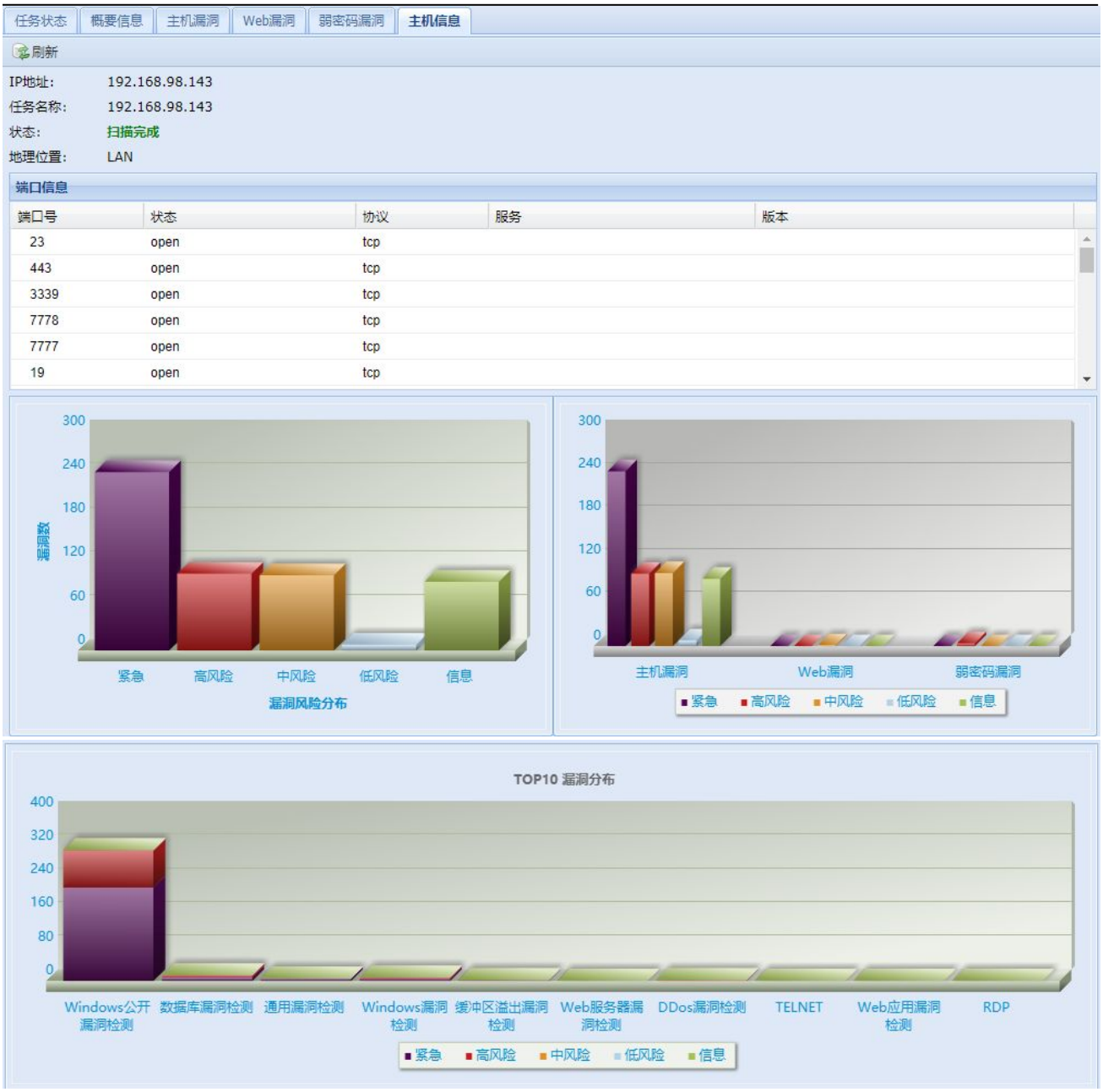
查看扫描任务的实时状态，您可以通过本页面查看到正在执行扫描中的网站扫描进度和相关的扫描信息。

- “刷新”：刷新记录（扫描显示的漏洞信息需点击刷新实时查看）。
- “任务状态”：该页面显示任务名称、状态、说明（地理位置及网站标题）、风险等级、漏洞统计等。
- “概要信息”：该页面显示扫描任务的信息。如任务名称、扫描 IP 数、扫描域名数、状态、域名列表、任务调度、开始和结束时间以及 TOP10 漏洞统计。

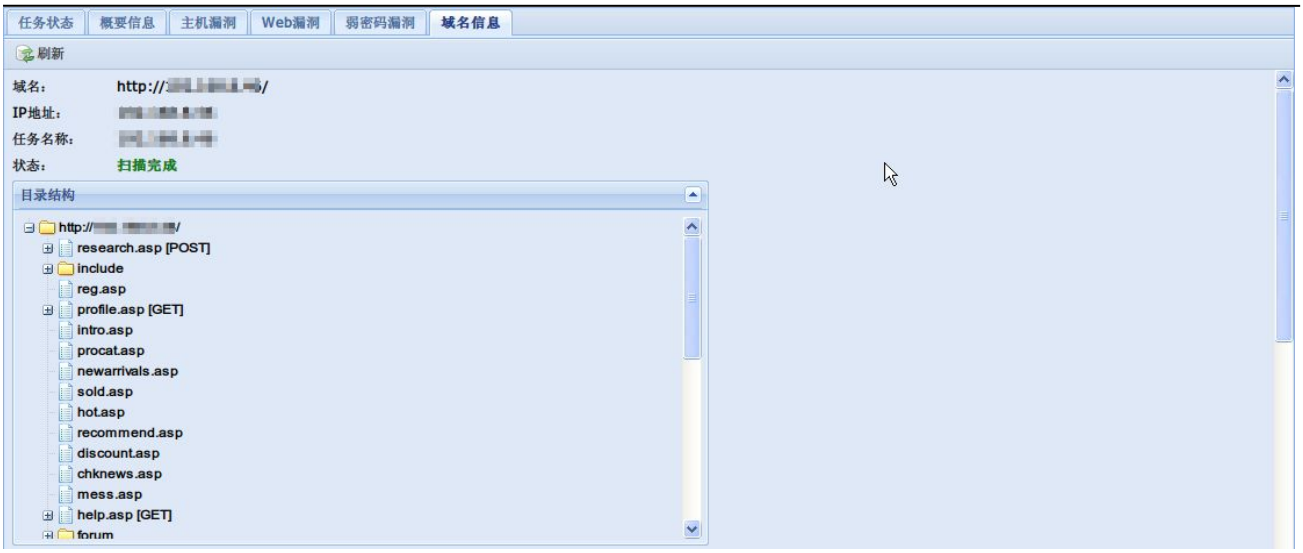


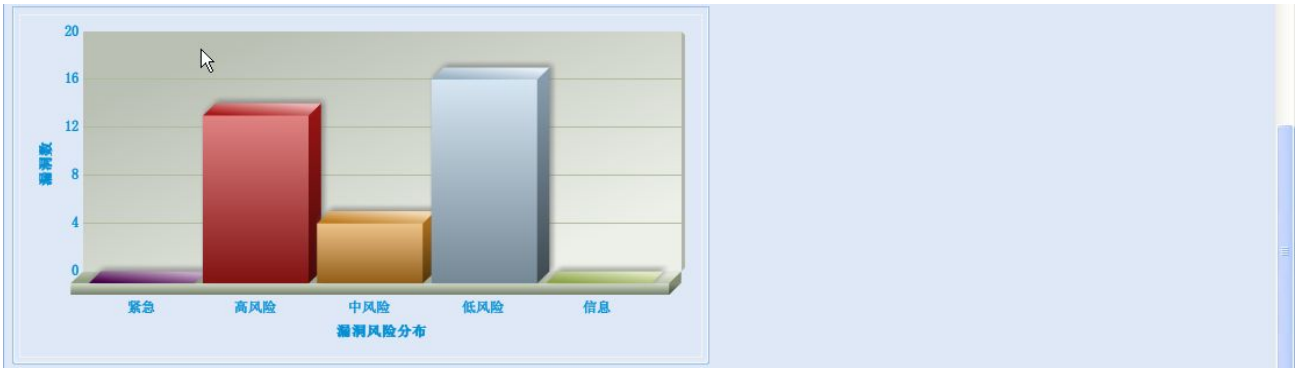


- “主机信息”：该页面显示该 IP 下的主机信息，包括扫描主机的状态、地理位置、操作系统、端口信息以及漏洞统计数。在“扫描详细信息”页面中的操作一栏，点击主机后的查看主机信息按钮，弹出“主机信息”页面。



- “域名信息”：该页面显示该 IP 下的域名信息，包括扫描域名的状态、目录结构、漏洞统计。在“扫描详细信息”页面中的操作一栏，点击域名后的查看域名信息按钮，弹出“域名信息”页面。

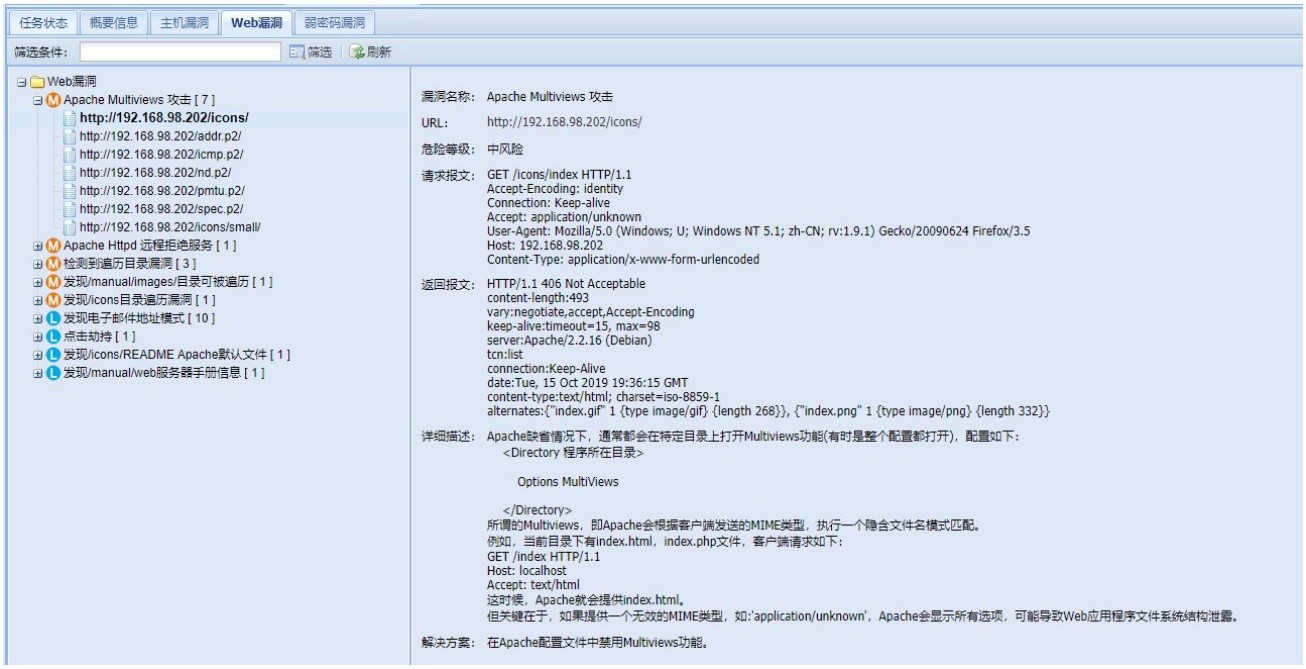




- “主机漏洞”：该页面显示任务扫描出的主机漏洞。页面左侧显示扫描的主机漏洞，单击 IP 后，右侧会显示该漏洞的描述和解决方案。

1. “筛选条件”：筛选出用户所需要 IP 的漏洞信息。输入 IP，点击筛选。点击【取消筛选】后，则显示该任务的所有主机漏洞。
2. “所有漏洞”：显示该任务的所有漏洞。
3. “可利用漏洞”：显示可以被成功利用的漏洞。

- “Web 漏洞”：该页面显示任务扫描出的 Web 漏洞。页面左侧显示扫描出的 Web 漏洞。如果单击域名后，右侧会显示该漏洞的描述信息和解决方案。

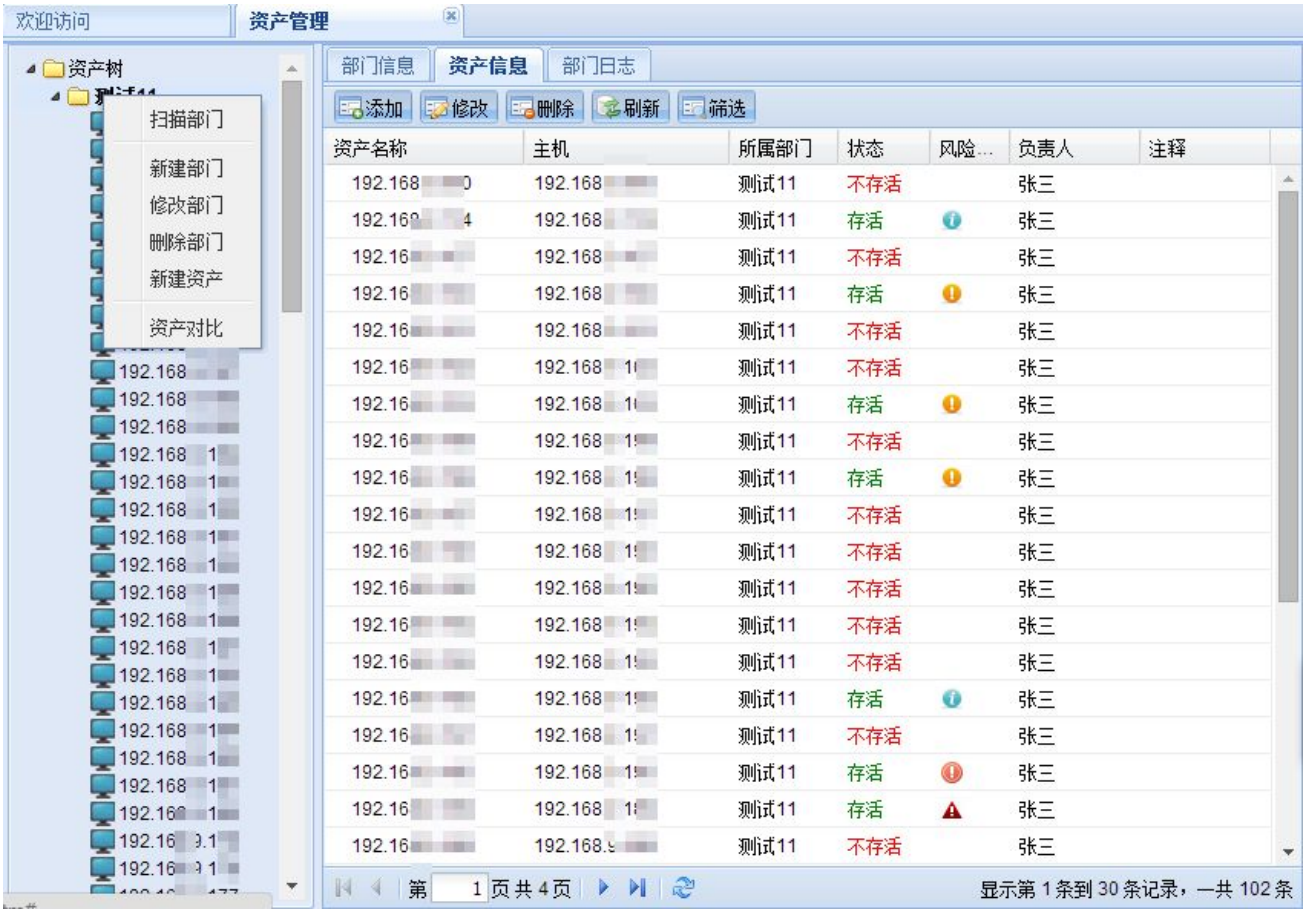


1. “筛选条件”：筛选出用户所需要的 IP 或域名的漏洞列表，内容输入 IP 或域名，点击筛选。点击【取消筛选】后，则显示该任务的所有 Web 漏洞。
2. 验证性扫描功能：通过对已扫到的 Web 漏洞进行验证，从而得到该网站路径、数据库版本、数据库表名……如上图，带有  的 URL 说明该漏洞经过验证性得到的扫描结果。

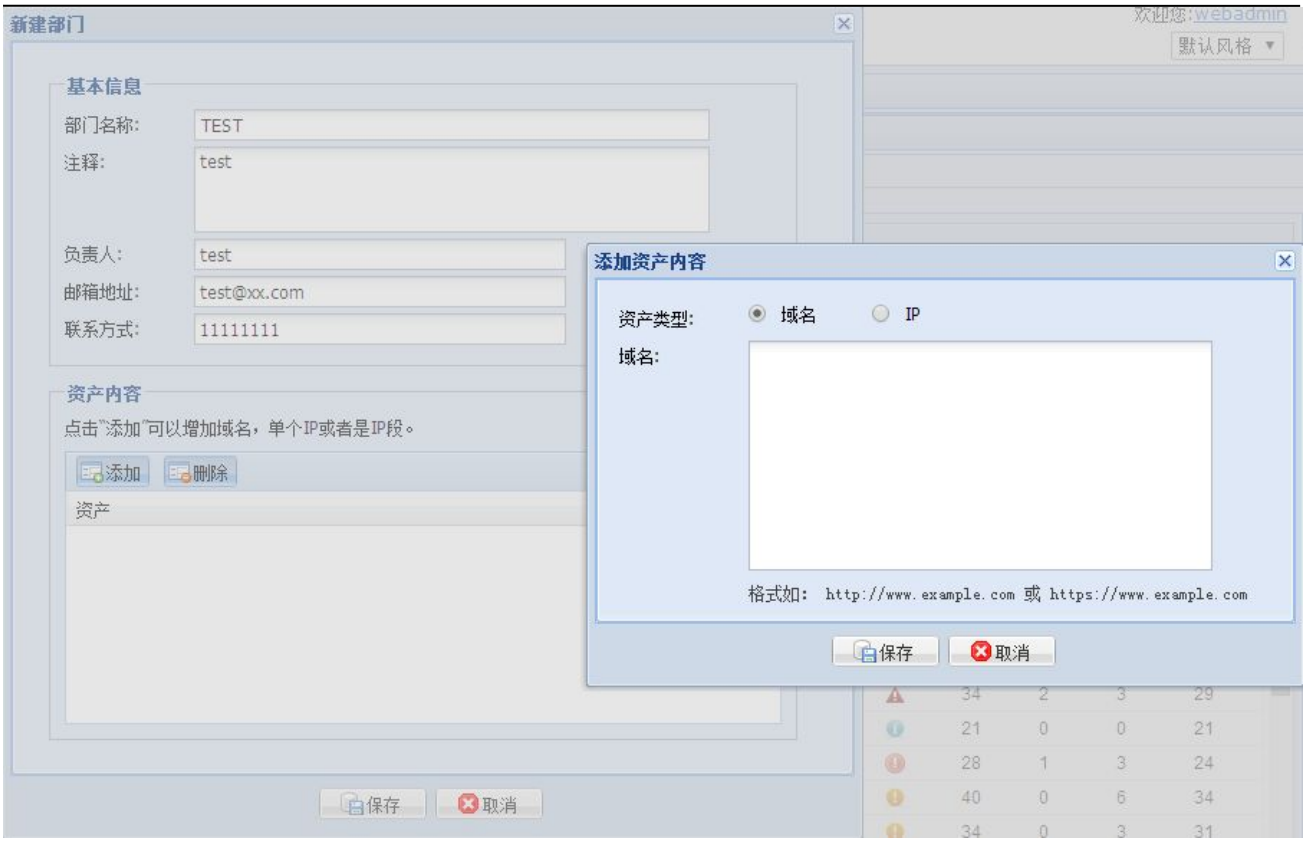
- “弱密码漏洞”：该页面显示任务扫描出的弱密码漏洞。

9、资产管理

对管理员所管理的资产进行分部门集中管理，便于漏洞扫描、漏洞修补以及资产对比；



- 新建部门：右击“部门”或“资产树”，选择“新建部门”。填写部门名称、注释、负责人、邮箱地址、联系方式以及添加资产内容后，点击【保存】按钮，新建部门成功。



- 新建资产：右击“部门”或“资产树”，选择“新建资产”。填写资产、资产名称、所属部门、资产类型、负责人、注释后，点击【保存】按钮，新建资产成功。

- 修改部门：右击“部门”，选择“修改部门”。修改部门名称、注释、负责人、邮箱地址、联系方式以及添加资产内容后，点击【保存】按钮，修改部门成功。

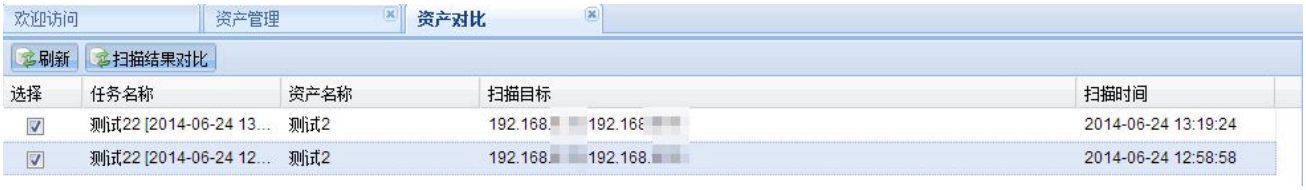
- 修改资产：右击“资产”，选择“修改资产”。修改资产、资产名称、所属部门、资产类型、负责人、注释后，点击【保存】按钮，修改资产成功。

- 删除部门：右击“部门”，选择“删除部门”，弹出“删除提示”，点击【是】按钮，删除部门成功

。

- 删除资产：右击“资产”，选择“删除资产”，弹出“删除提示”，点击【是】按钮，删除资产成功。

- 资产对比：右击“部门”或“资产”，选择“资产对比”，弹出“资产对比”页面，勾选两条扫描结果，点击【扫描结果对比】按钮；弹出“扫描结果对比”页面，显示两个部门的扫描结果。（注：扫描对比是指对同个资产或部门在不同时间段的扫描结果进行资产对比；扫描结果对比中不通漏洞名称处则以红色字体表示）



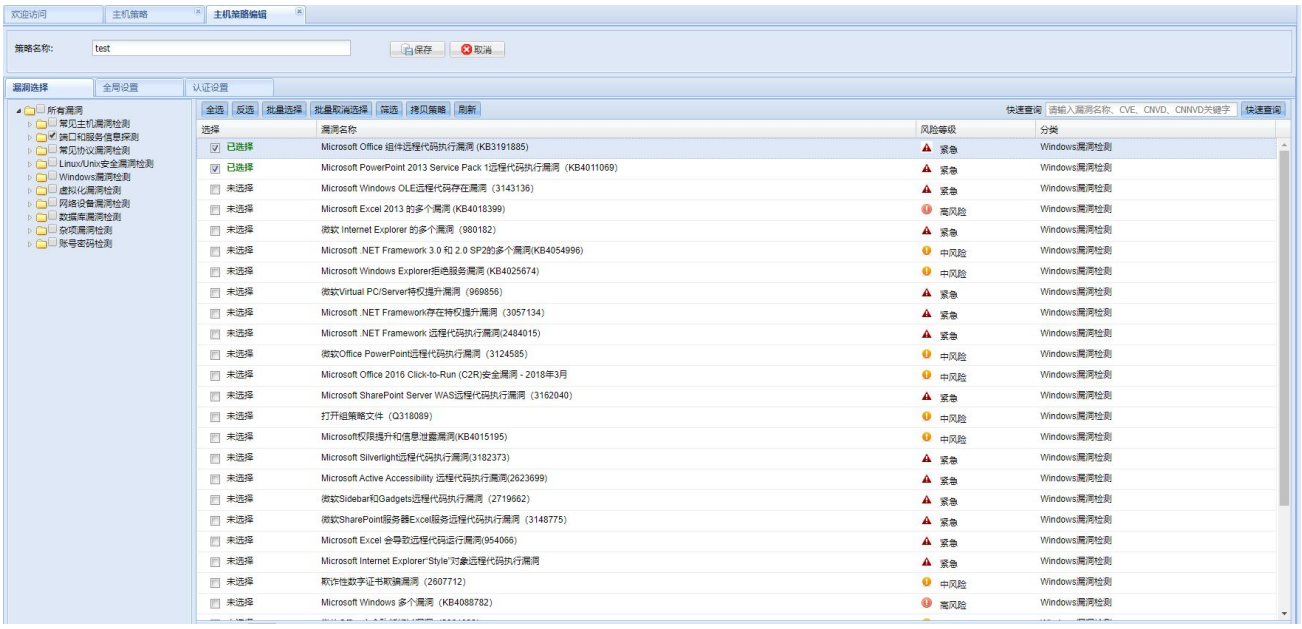

扫描结果对比
资产扫描信息
扫描时间:
2014-06-24 12:58:58
漏洞数:
128
资产范围:
192.168
192.168.
扫描时间:
2014-06-24 13:19:24
漏洞数:
127
资产范围:
192.168
192.168
查看
刷新
漏洞名称【扫描时间：2014-06-24 12:58:58】
漏洞名称【扫描时间：2014-06-24 13:19:24】
Windows Local Security Authority Service远程缓冲区溢...
Windows Local Security Authority Service远程缓冲区溢
Microsoft SMB远程缓冲区溢出漏洞
Microsoft SMB远程缓冲区溢出漏洞
Microsoft Windows DCOM RPC接口长主机名远程缓冲...
Microsoft Windows DCOM RPC接口长主机名远程缓冲
Microsoft Windows ASN.1库BER解码堆破坏漏洞（MS0...
Microsoft Windows ASN.1库BER解码堆破坏漏洞（MS
SMB 中的漏洞可能允许远程执行代码（MS09-001）
SMB 中的漏洞可能允许远程执行代码（MS09-001）
Microsoft COM Internet Services (CIS) RPC Over HTTP...
Microsoft COM Internet Services (CIS) RPC Over HTTI
Windows Server服务 RPC请求缓冲区溢出漏洞(MS08-0...
Windows Server服务 RPC请求缓冲区溢出漏洞(MS08-
分布式事务处理协调器存在拒绝服务漏洞（MS06-018）
分布式事务处理协调器存在拒绝服务漏洞（MS06-018）
Microsoft Windows NetDDE远程任意指令执行漏洞(MS0...
Microsoft Windows NetDDE远程任意指令执行漏洞(MS
取消

10、策略管理

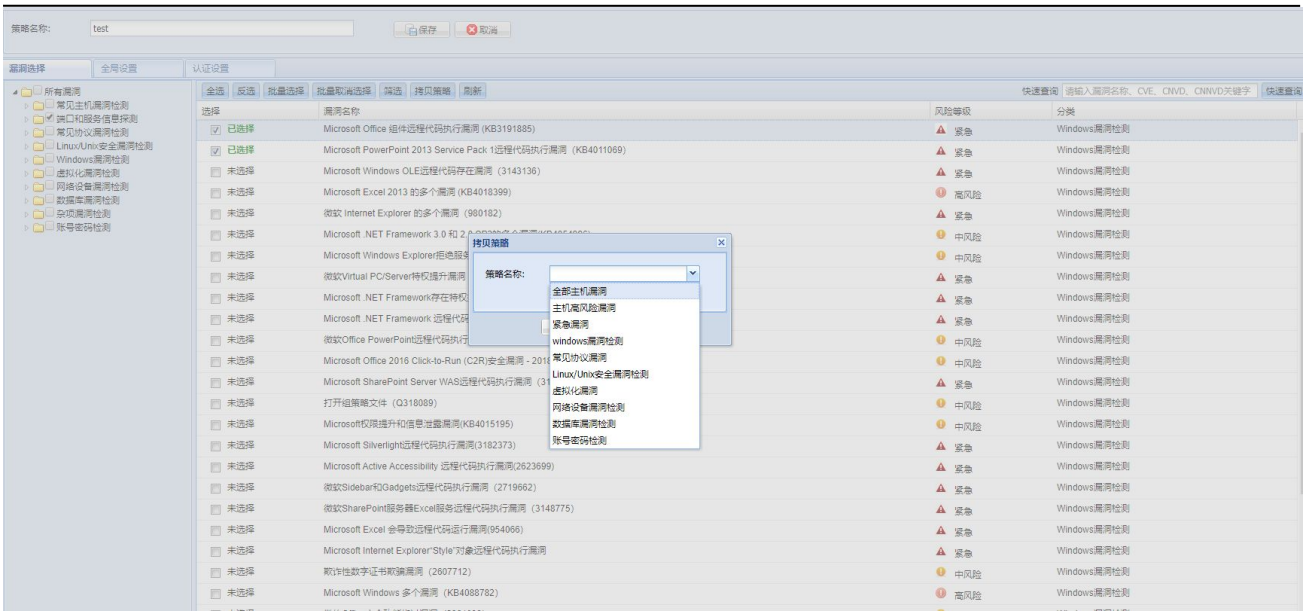
主机策略

管理漏洞扫描的主机策略，可以通过添加或删除主机扫描策略对需扫描的网站进行针对主机漏洞的扫描。

- 添加策略：单击【添加】按钮，弹出“主机策略编辑”页面，添加策略名称，可以选择漏洞类型，在复选框中打钩选择漏洞，最后保存，添加成功。

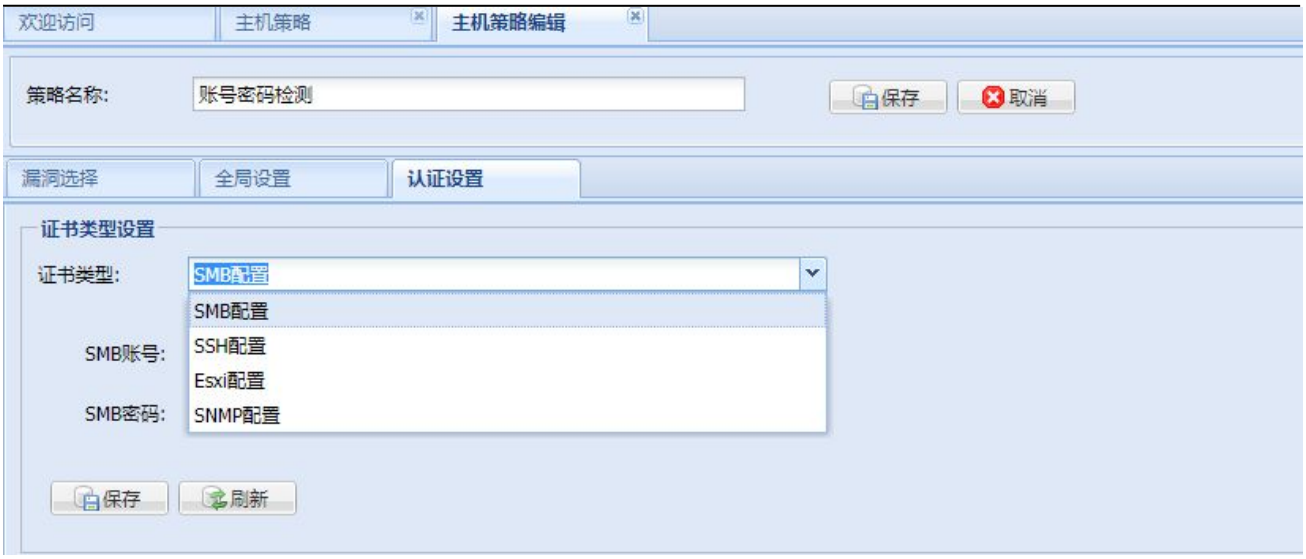


1. 【全选】：单击【全选】按钮，所有漏洞全部勾选。
2. 【反选】：单击【反选】按钮，勾选未被选中的漏洞。
3. 【批量选择】：使用 shift 进行多选漏洞后，单击【批量选择】按钮，勾选选中的漏洞。
4. 【批量取消选择】：使用 shift 进行多选已勾选的漏洞后，单击【批量取消选择】按钮，取消已选择地漏洞。
5. 【拷贝策略】：单击【拷贝策略】按钮，选择需拷贝的策略类型。

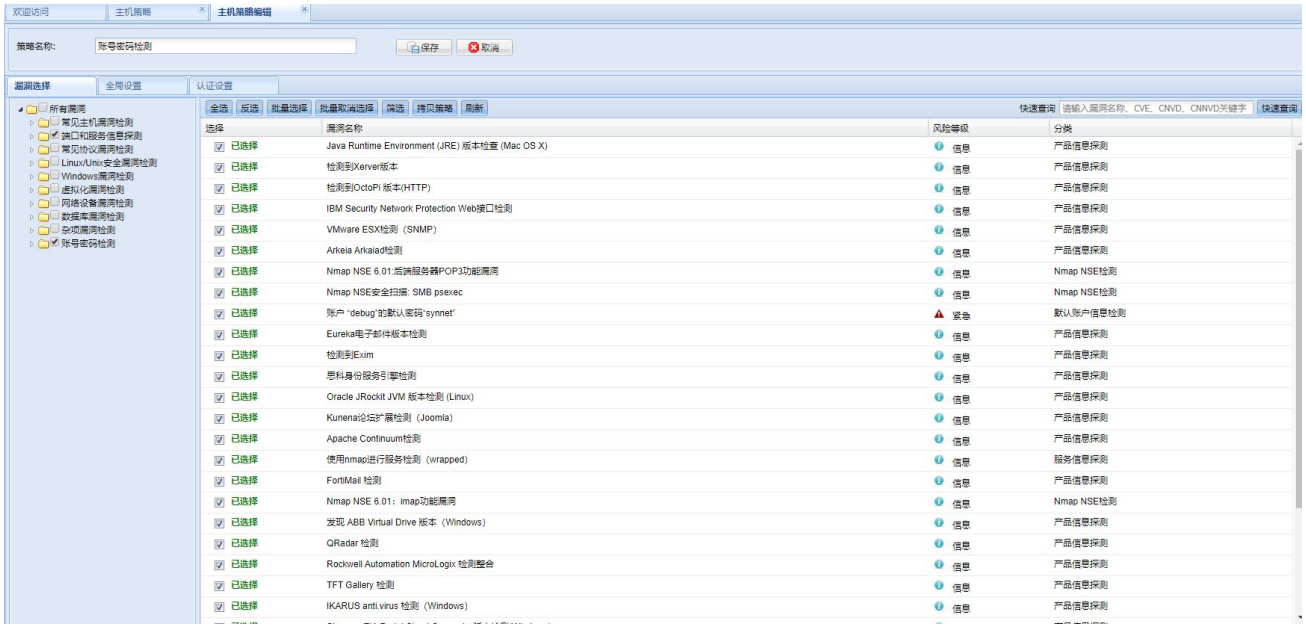


6. 【全局设置】：全局设置扫描任务的并发数、规则扫描并发数，扫描速度优化、安全检查、禁止扫描非开放 TCP 端口、禁止扫描非开放 UDP 端口。如图所示。

7. 【认证设置】：配置 SMB、SSH、Exsi、SNMP 登录性扫描。如图所示。



- 修改策略：单击【修改】按钮，弹出“主机策略编辑”对话框，修改策略名称，修改选择的漏洞，最后保存，修改成功。



- 删除策略：选择一条策略，单击【删除】按钮，弹出“删除提示”对话框，单击【是】，成功删除。

主机策略配置项

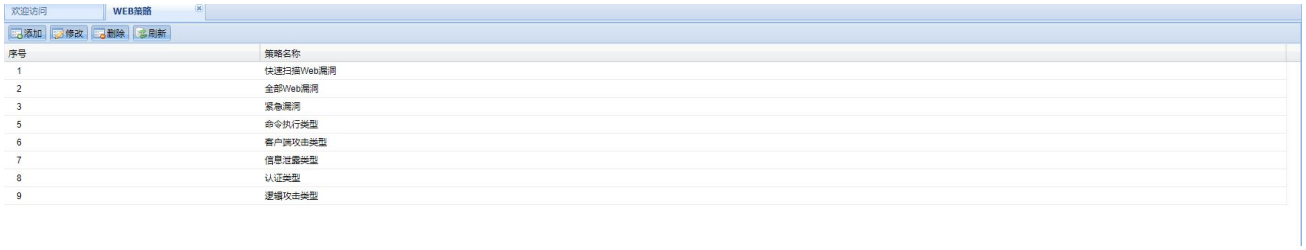
管理主机漏洞的扫描策略，可以通过添加配置项，针对特定的主机进行扫描。

提示：

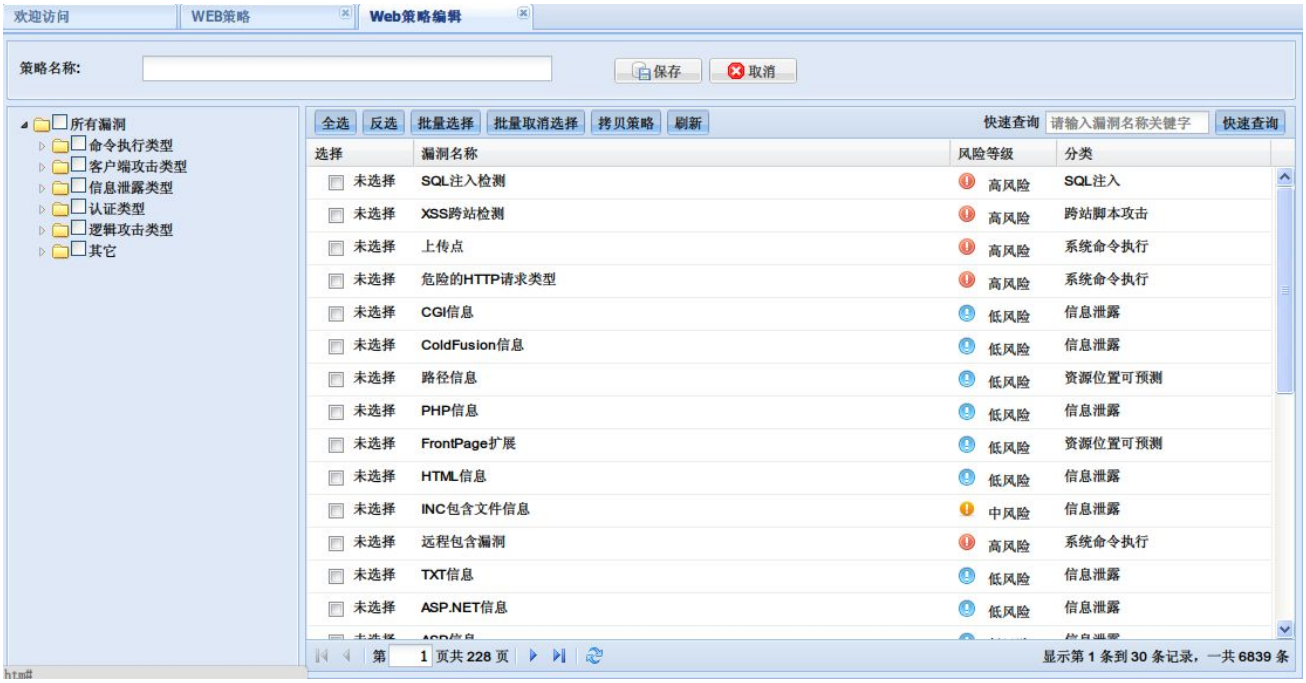
系统内置的主机扫描策略不能被删除。

WEB 策略

管理 web 漏洞扫描策略，你可以通过添加或修改扫描策略，对需要扫描的网站进行针对特定 web 漏洞的扫描。



- 添加策略：单击【添加】按钮，弹出“WEB 策略编辑”窗口，添加策略名称，可以选择漏洞类型，在复选框中打钩选择漏洞，最后保存，添加成功。



1. 全选：单击【全选】按钮，所有漏洞全部勾选。
2. 反选： 单击【反选】按钮，选中的漏洞取消勾选，未被选中的漏洞。
3. 【批量选择】：使用 shift 进行多选漏洞后，单击【批量选择】按钮，勾选选中的漏洞。
4. 【批量取消选择】：使用 shift 进行多选已勾选的漏洞后，单击【批量取消选择】按钮，取消已选择地漏洞。
5. 【拷贝策略】：单击【拷贝策略】按钮，选择需拷贝的策略类型。

- 修改策略：单击【修改】按钮，弹出“WEB 策略编辑”对话框，修改策略名称，修改选择的漏洞，最后保存，修改成功。

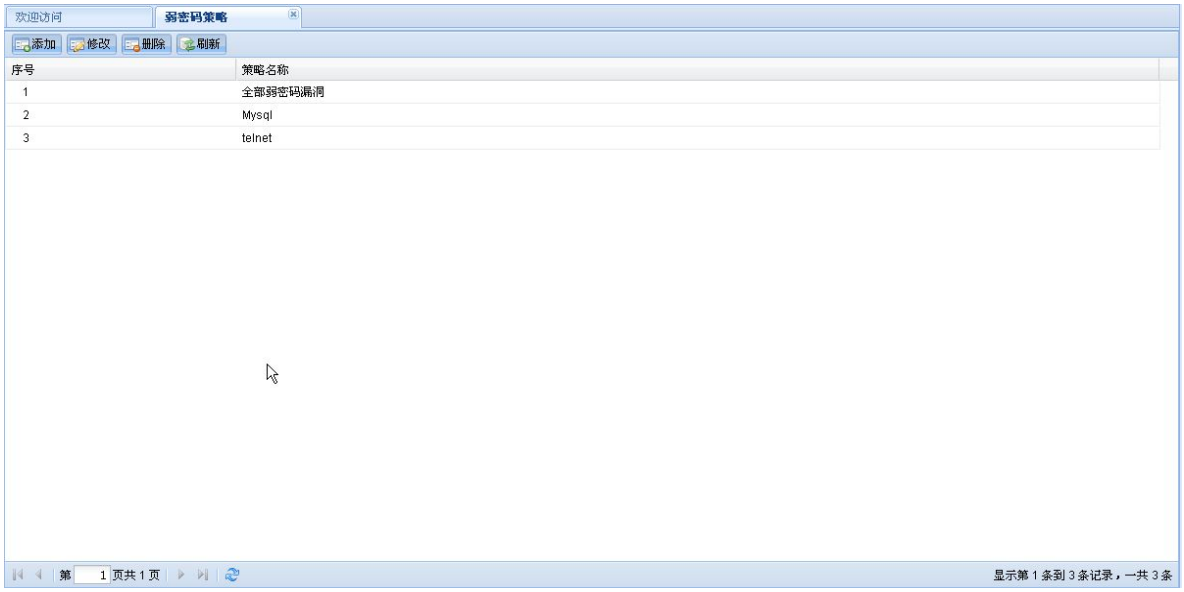
- 删除策略：选择一条策略，单击【删除】按钮，弹出“删除提示”对话框，单击【是】，成功删除。

提示：

系统内置的 Web 漏洞扫描策略，不能被删除。

弱密码策略

- 管理弱密码漏洞扫描策略，你可以通过添加或更新扫描策略，对需要扫描的网站进行针对特定弱密码漏洞的扫描。



- 添加策略：单击【添加】按钮，弹出“弱密码策略-添加”对话框，添加策略名称，可以选择漏洞类型，在复选框中打钩选择漏洞，修改弱密码对应端口号，最后保存，添加成功。

- 修改策略：单击【修改】按钮，弹出“弱密码策略-修改”对话框，修改策略名称，修改选择的漏洞，最后保存，修改成功。

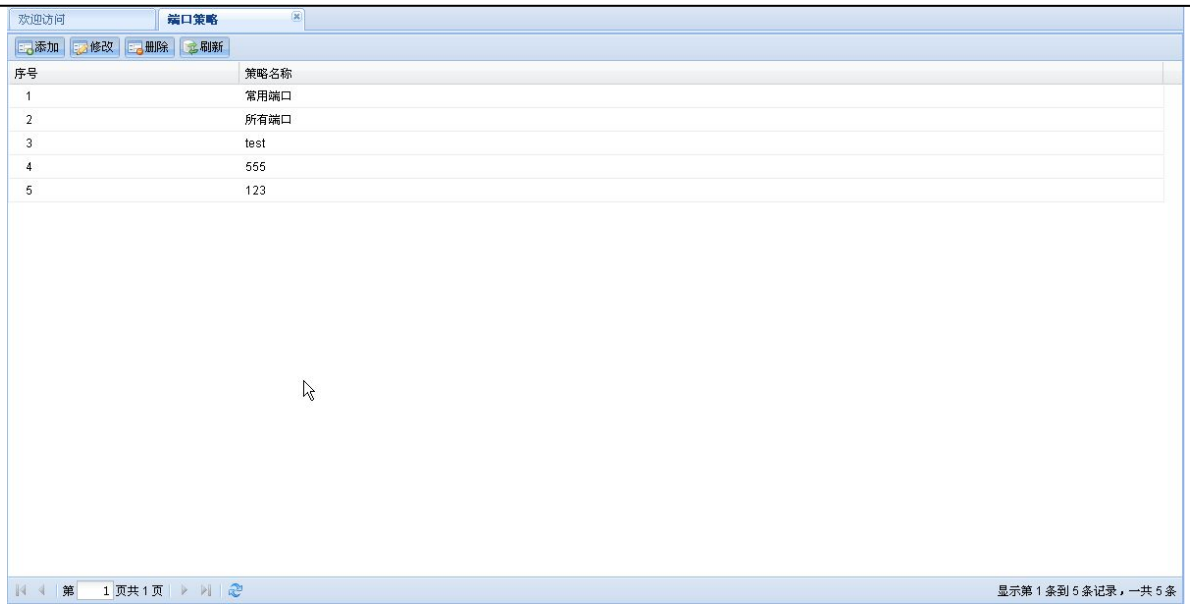
- 删除策略：选择一条策略，单击【删除】按钮，弹出“删除提示”对话框，单击【是】，成功删除。

提示：

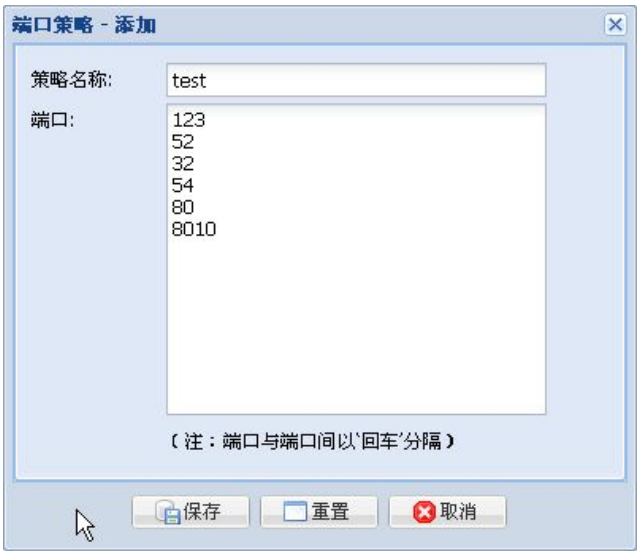
系统内置的弱密码扫描策略，不能删除。

端口策略

该页面设置扫描端口，用来在详细扫描中添加所需扫描的端口。



- 【添加】：单击【添加】按钮，弹出“端口策略-添加”页面，添加新的端口策略，最后点击【保存】，添加成功。



- 【修改】：选择所需修改的端口策略，单击【修改】按钮，弹出“端口策略-修改”页面，修改端口策略，最后点击【保存】，修改成功。

- 【删除】：选择所需删除的端口策略，单击【删除】按钮，弹出“删除提示”对话框，单击【是】，成功删除策略。

提示：

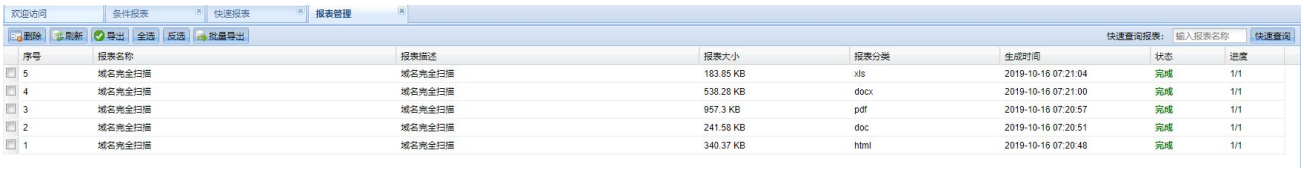
默认的常用端口不可删除。

11、报表管理

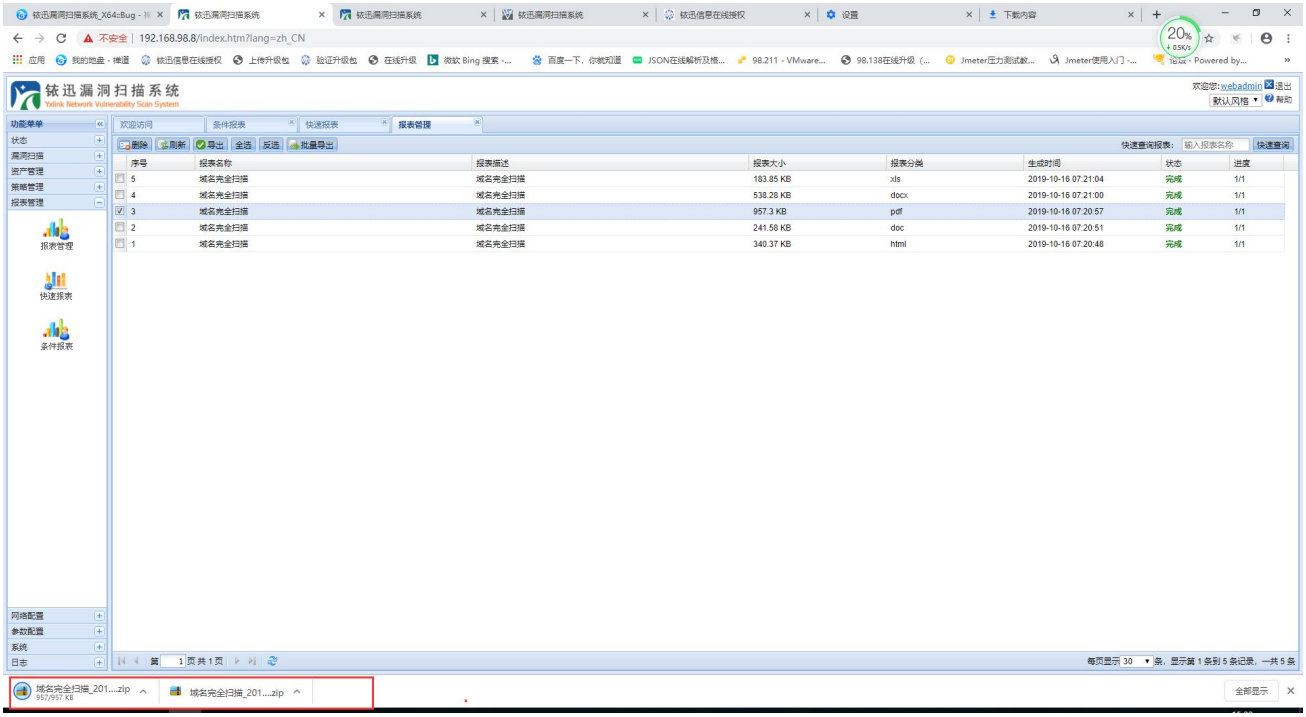
该模块提供生成 HTML、PDF、DOC、DOCX 格式报表的功能，可以对生成的报表进行导出、删除等操作。

报表管理

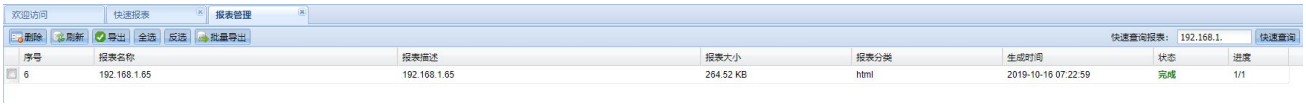
该页面显示生成的报表，用户可以根据需要导出报表，删除报表，或者进行快速查询。



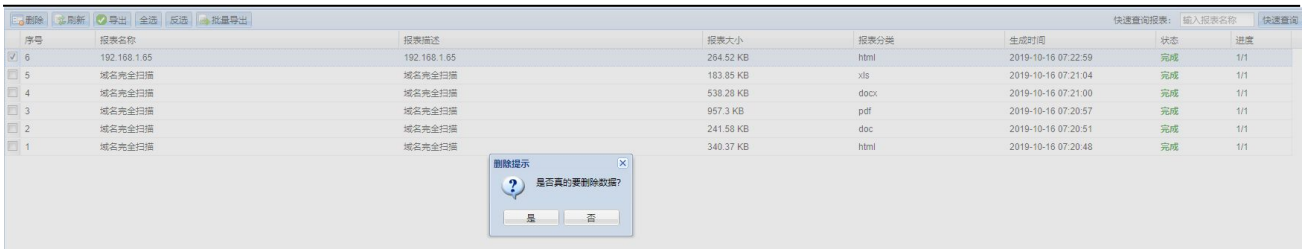
- 选择一条报表，点击【导出】或双击一条报表，即可将报表下载到本地。



- 输入报表名称，点击【快速查询】，可以进行报表的快速查询

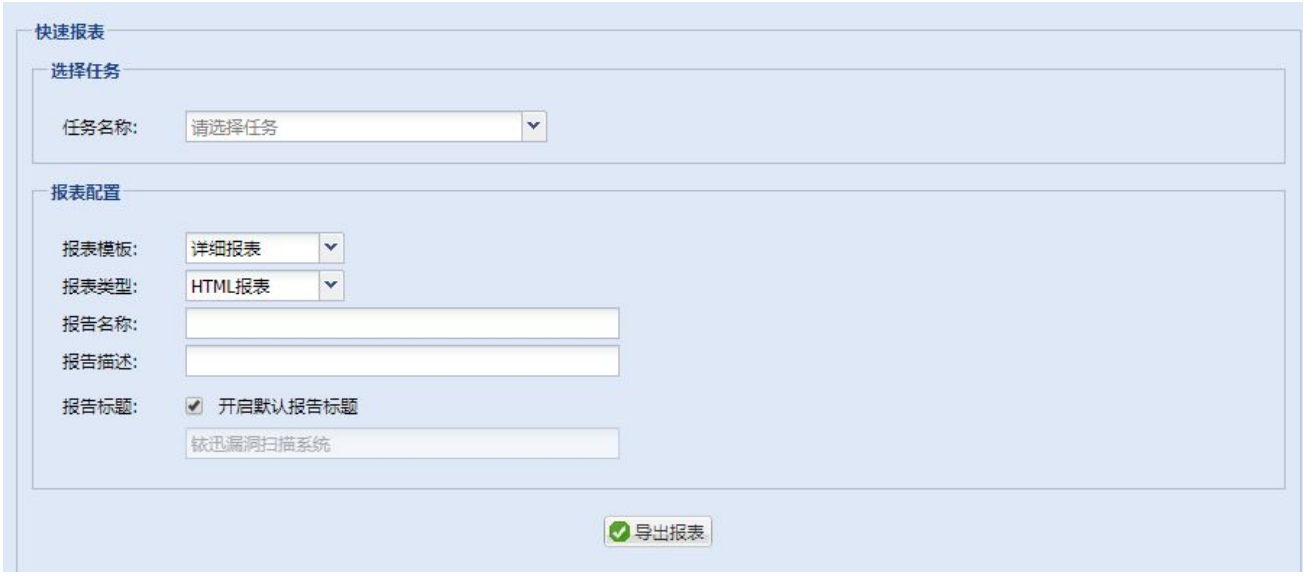


- 选择一条或多条报表，点击【删除】，可以删除报表



快速报表

该页面能够按照选择的扫描任务和输出格式，生成对应格式的报表。



- 选择任务：通过下拉框选择需要生成报表的扫描任务。
- 报表配置：提供对“报表类型”、“报表名称”、“报表描述”进行选择和输入。

⚠注意:

点击【导出报表】按钮后，系统会在后台自动生成报表，状态可在报表管理中刷新查看。

条件报表

该页面可以通过选择的扫描任务、报表条件、输出的格式来生成相应的报表。

- 选择任务：通过下拉框选择需要生成报表的扫描任务。
- 报表条件：按需求选择需要生成的扫描内容。
- 报表配置：提供对“报表类型”、“报表名称”、“报表描述”进行选择和输入。

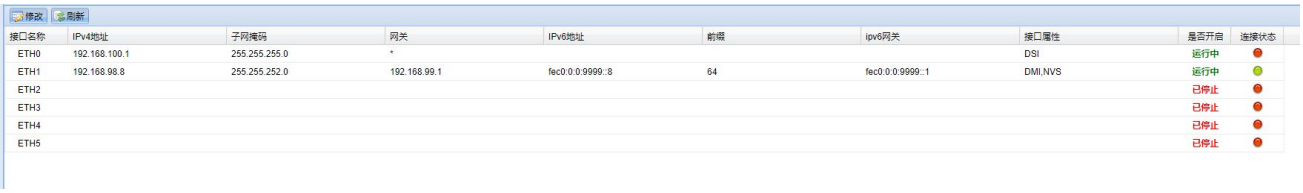
提示：

报表条件中勾选的扫描内容不同，显示的结果不同（如：只勾选弱密码时，只会显示弱密码类型）

12、网络配置

网络接口

该页面列出了设备所有网络接口的工作状态，包括 IP 地址、子网掩码、网关、是否启用、工作方式、接口属性等信息。



选择某个网络接口，点击【修改】，弹出【网络接口-修改】对话框，对该网络接口进行配置。

配置网络接口为普通方式

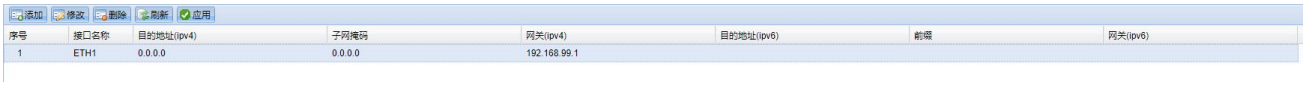
1. 双击需要修改的网络接口，比如：ETH4，弹出【网络接口-修改】对话框；
2. 选择接口状态为“启用”；
3. 填写“IP 地址”，“子网掩码”；
4. 如果该接口有相应的网关，请填写网关。如果没有，可以留空不填写。
5. 点击【应用】按钮，该设置生效并返回上一级页面。

ⓘ提示：

配置 IPV6 地址与 IPV4 配置方法相同，根据用户环境输入 IPv6 地址、前缀与 IPv6 网关即可。如图所示。

静态路由

用于配置系统当前的静态路由表，具体界面如下图。您可以添加、修改、删除静态路由。配置完成后，必须点击【应用】按钮以便使配置生效。



只能为工作于普通方式的网络接口配置静态路由。

修改默认路由

例如：

1. 序号为 1 的记录为默认路由，双击该记录，弹出“静态路由-修改”对话框；

2. 选择“接口名称”：即对应的网络接口名称，可以修改默认路由所在的接口，比如从 ETH4 改到 ETH3；
3. 勾选“设置为默认路由”；
4. 填写“网关（ipv4）”，这里添加的网关必须与【网络接口】页面中该网络接口的网关一致。并且默认路由的网关不能为空；
5. 点击【保存】按钮，返回上一级页面；

提示：

配置 IPv6 相关的默认路由，根据用户环境输入目的地址（IPv6）、前缀与网关（IPv6）即可。如图所示。

⚠注意：

系统只能有一条默认路由，可以修改默认路由，但不能添加多条默认路由。

DNS 设置

设置 DNS 服务器地址，系统的邮件通知、漏洞扫描等功能依赖于 DNS 设置，因此建议您最好配置 DNS 服务器地址。

ⓘ提示：

如果您不清楚 DNS 服务器地址，请联系网络管理员获得。

接口管理

此处提供系统初始化接口（DSI），设备管理接口（DMI），设备扫描接口（NVS）的接口配置功能。

配置系统初始化接口（DSI）

DSI 是初始化接口，在设备初始配置时使用。如果一个网络接口的接口属性被配置为 DSI，通常简称为 DSI 接口，该接口的工作模式和接口属性都不能被修改。

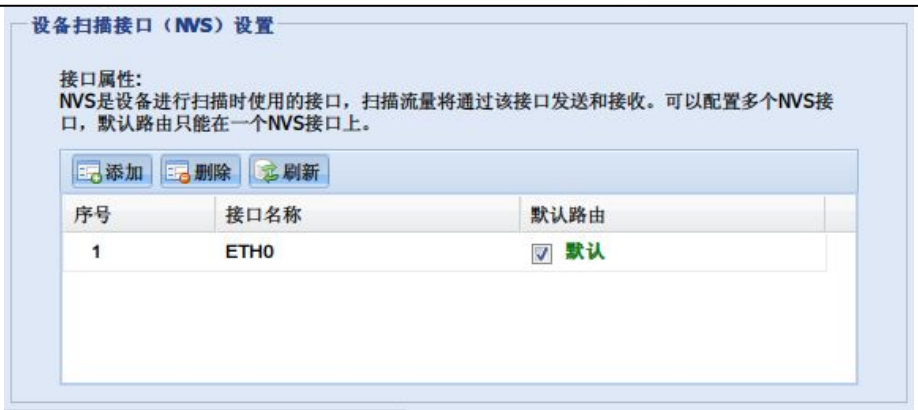
DSI 接口提供 DHCP 服务，IP 为固定 IP，不可以被修改，DHCP 分配的 IP 段 192.168.100.10-192.168.100.100。

配置设备管理接口（DMI）

DMI 是设备管理接口，通过该接口访问设备的管理页面。如果一个网络接口的接口属性被配置为 DMI，通常简称为 DMI 接口。

配置设备扫描接口（NVS）

NVS 是设备扫描接口，扫描流量将通过该接口发送和接收。可以配置多个 NVS 接口，默认路由只能在一个 NVS 接口上。



⚠注意：

只有工作模式为普通，且不是 DSI 接口的网络接口才能配置为管理接口。

系统允许配置多个设备管理接口。

设备扫描接口的默认路由有且只有一个。

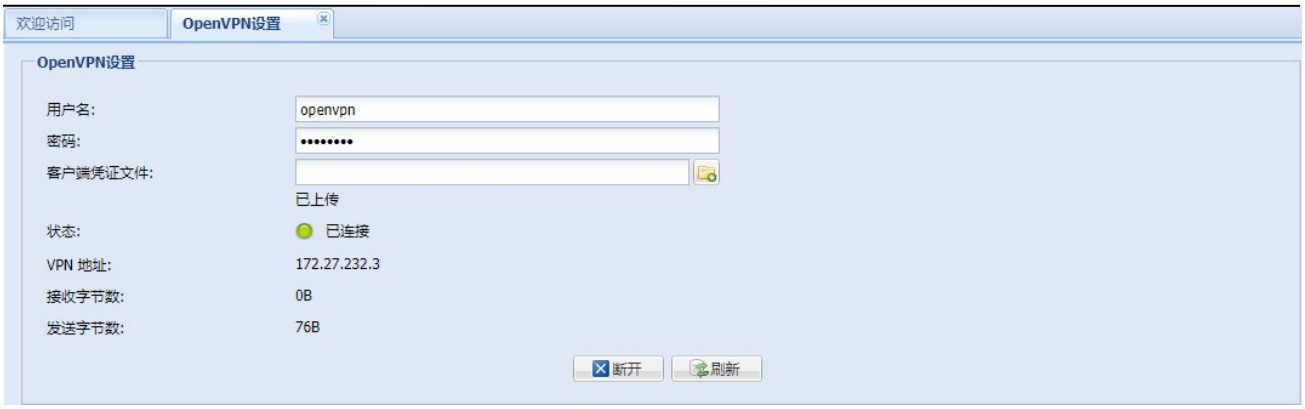
VPN 设置

该模块可以提供设备连接 VPN 的功能，方便您扫描您的内部网站。也可以在扫描网站时，隐藏设备自身的网络 IP 地址，提高安全系数。

- VPN 设置：填写正确的 VPN 信息，包括” IP 地址“、“用户名”和“密码”。填写正确后可以点击保存进行保存设置，也可以直接进行连接的操作。
- VPN 状态：可以实时的反应当前 VPN 连接的状态。

OpenVPN 设置

该模块可以提供设备连接 OpenVPN 的功能，方便您扫描您的内部网站。也可以在扫描网站时，隐藏设备自身的网络 IP 地址，提高安全系数。



- OpenVPN 设置：填写正确的 OpenVPN 信息，包括“用户名”、“密码”和“客户端凭证文件”。填写正确后可以点击保存进行保存连接操作。
- OpenVPN 状态：可以实时的反应当前 VPN 连接的状态。
- VPN 地址：连接成功后，展示 VPN 地址。
- 接收字节数：VPN 连接成功后、使用过程中接收的字节数。
- 发送字节数：VPN 连接成功后、使用过程中发送的字节数。

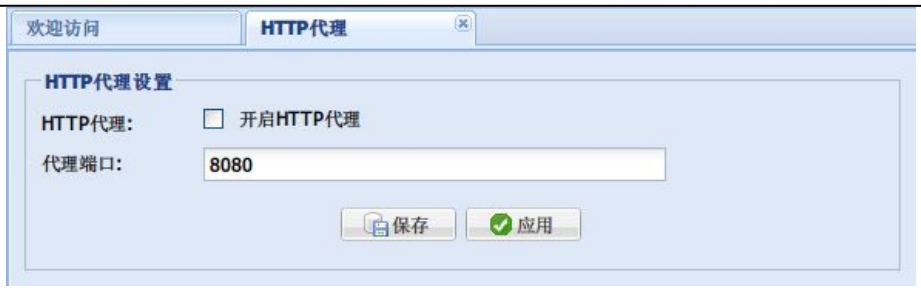
Socks 代理

该模块提供 Socks 代理，通过代理 IP 地址和代理端口来扫描另一网络中的内部主机和网站。

- Socks 代理设置：填写正确的代理 IP 地址以及代理端口，填写正确后可以点击保存进行保存设置，也可以直接进行应用的操作。

HTTP 代理

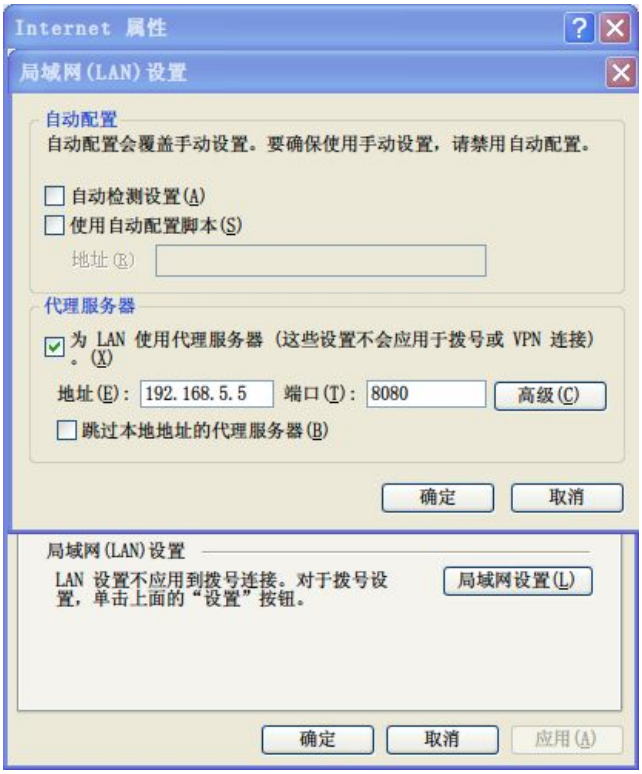
该模块通过开启 HTTP 代理端口，提供 HTTP 代理服务器的功能。用来获取通过用户名和密码登录时的 cookie，从而进行登录扫描。



示例：www.renren.com

步骤：

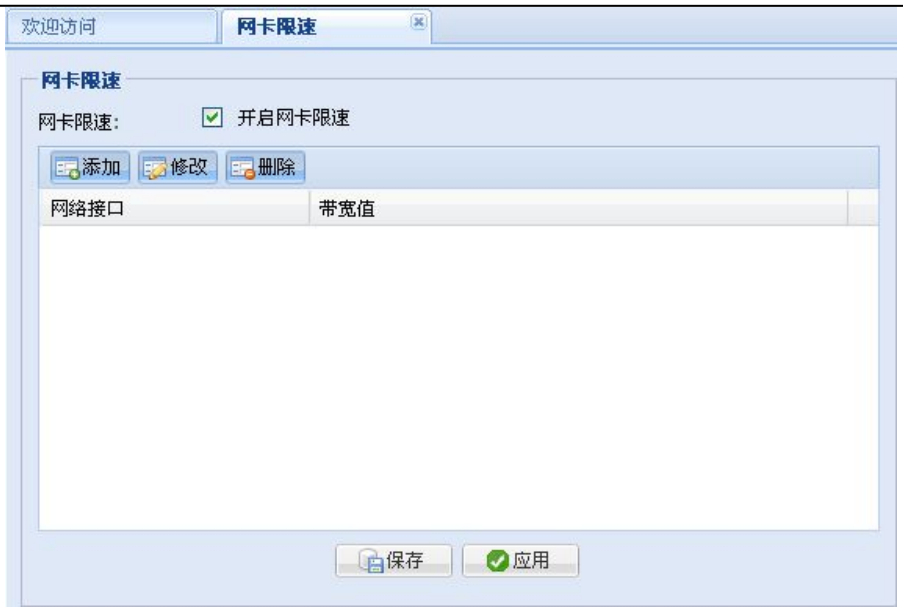
1. 开启 HTTP 代理，设置代理端口，如 8080 端口；
2. 在本地浏览器进行设置“Internet 属性”，选择“连接”选项卡；
3. 点击“局域网设置”，弹出“局域网（LAN）设置”界面，在“代理服务器”中勾选复选框“为 LAN 使用代理服务器”，地址设置为漏扫 DMI 口的 IP 地址，端口为 8080，点击确定；



4. 登录 www.renren.com，输入用户名和密码登录人人网后关闭网页，并重复上一步步骤，将“为 LAN 使用代理服务器”复选框勾除，点击确定；
5. 新建“登录扫描”这个任务，在“添加扫描目标”的扫描类型选择“登录扫描”，填写域名：www.renren.com，填写登录 URL：www.renren.com，在导入 Cookie 的下拉框中选择 Cookie，点击保存，任务新建完成并执行扫描。

网卡限速

设置对网络接口的所能使用的最大带宽，防止扫描器占用过多的带宽，影响网络正常的使用。

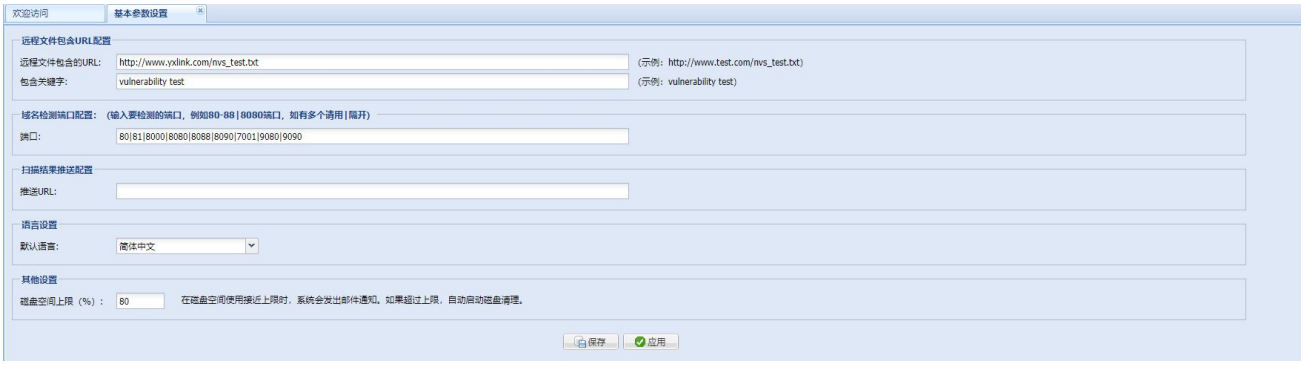


网卡限速：添加网络接口，设置该接口的带宽值。

13、参数设置

基本参数设置

本页面设置远程文件包含 URL 以及域名检查端口。



- 远程文件包含 URL 配置： 在进行远程文件包含的规则检测时，会在请求指定 URL 的参数中加入设定的远程 URL，在返回内容中查找指定的关键字。
- 域名检测端口配置：探测需要扫描的 IP 地址的指定端口是否运行 HTTP 服务。
- 扫描结果推送配置：扫描任务的结果发送到配置的 URL。
- 语言设置：设置系统使用简体中文或 English。
- 其他设置：设置磁盘使用上限，触发上限值时、发送邮件通知，超过上限，系统自动清理磁盘。

通知设置

本页面设置用于发送通知邮件的邮箱信息，包括发送邮件的 SMTP 服务器信息，以及接收通知的邮箱地址。

通知邮箱设置：

- 发件人邮箱： 用于发送邮件的邮箱。
- 发件人账号： 用于发送邮件的账号名称。
- 发件人密码： 用于发送邮件的邮箱密码。
- SMTP 服务器地址： 用于发送邮件的 SMTP 服务器地址。

- SMTP 服务器端口： 用于发送邮件的 SMTP 服务器端口。
- 收件人邮箱： 用于接收通知邮件的邮箱。

提示：

当本设备磁盘空间使用率接近设置上限的 90%的时候，本设备将自动发送邮件提醒管理员。

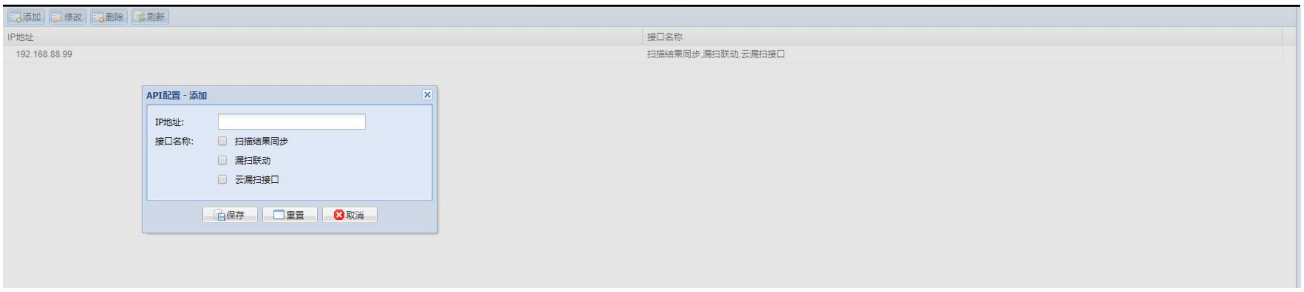
syslog

syslog 常被称为系统日志或系统记录，是一种用来在互联网协议（TCP/IP）的网络中传递存档信息的标准。本系统支持 syslog 日志的发送。

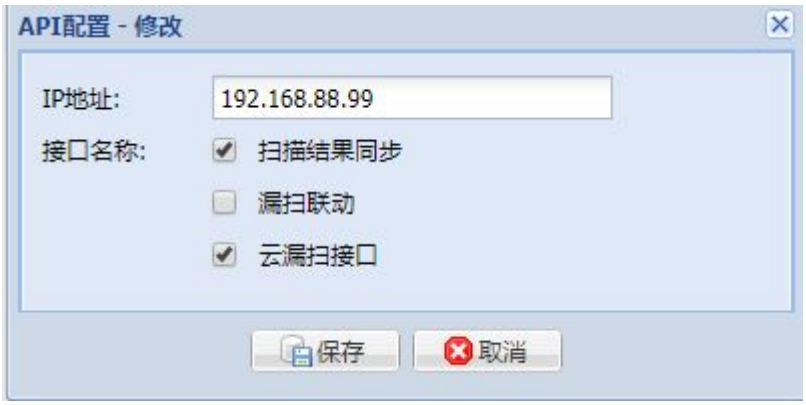
API 配置

API 是一些预先定义的函数，目的是提供应用程序与开发人员基于某软件或硬件得以访问一组例程的能力，而又无需访问源码，或理解内部工作机制的细节。

- 添加 API：点击【添加】、弹出“API-添加”对话框，用户根据需求输入 IP 地址、选择“接口名称”，如图所示。

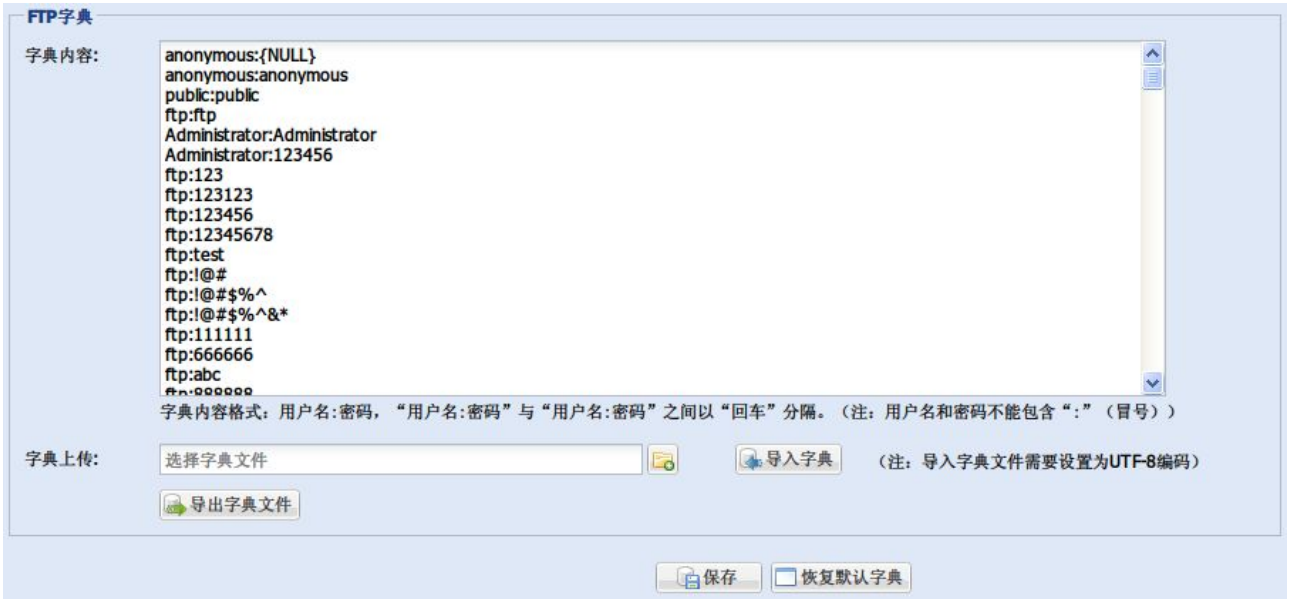


- 修改 API：选择新增的 API 配置、点击【修改】，根据需求修改配置，保存即可。如图所示。



FTP 字典

FTP 字典中包含使用 FTP 时可能经常使用的用户名及密码，弱密码扫描利用该字典进行探测。



- 字典内容：可添加用户名与密码，格式为“用户名：密码”，中间用冒号（：）分割，每条字典记录独立一行。用户名和密码不能包含冒号。
- 字典上传：选择密码库上传，格式与字典内容格式相同，扩展名为 dic 文件
- 【导入字典】：点击导入，字典文件上传。
- 【导出字典文件】：点击链接下载字典内容
- 【保存】：点击【保存】按钮，保存添加的字典内容。

- 【恢复默认字典】：恢复最初始的字典。

MYSQL 字典

MYSQL 字典中包含使用 MYSQL 时可能经常使用的用户名及密码，弱密码扫描利用该字典进行探测。

- 字典内容：可添加用户名与密码，格式为“用户名：密码”，中间用冒号（：）分割，每条字典记录独立一行。用户名和密码不能包含冒号。
- 字典上传：选择密码库上传，格式与字典内容格式相同，扩展名为 dic 文件
- 【导入字典】：点击导入，字典文件上传。
- 【导出字典文件】：点击链接下载字典内容
- 【保存】：点击【保存】按钮，保存添加的字典内容。
- 【恢复默认字典】：恢复最初始的字典。

MSSQL 字典

MSSQL 字典中包含使用 MSSQL 时可能经常使用的用户名及密码，弱密码扫描利用该字典进行探测。

- 字典内容：可添加用户名与密码，格式为“用户名：密码”，中间用冒号（：）分割，每条字典记录独立一行。用户名和密码不能包含冒号。
- 字典上传：选择密码库上传，格式与字典内容格式相同，扩展名为 dic 文件
- 【导入字典】：点击导入，字典文件上传。
- 【导出字典文件】：点击链接下载字典内容
- 【保存】：点击【保存】按钮，保存添加的字典内容。
- 【恢复默认字典】：恢复最初始的字典。

ORACLE 字典

ORACLE 字典中包含使用 ORACLE 时可能经常使用的用户名及密码，弱密码扫描利用该字典进行探测。

- 字典内容：可添加用户名与密码，格式为“用户名：密码”，中间用冒号（：）分割，每条字典记录独立一行。用户名和密码不能包含冒号。
- 字典上传：选择密码库上传，格式与字典内容格式相同，扩展名为 dic 文件
- 【导入字典】：点击导入，字典文件上传。
- 【导出字典文件】：点击链接下载字典内容
- 【保存】：点击【保存】按钮，保存添加的字典内容。
- 【恢复默认字典】：恢复最初始的字典。

TELNET 字典

TELNET 字典中包含使用 TELNET 时可能经常使用的用户名及密码，弱密码扫描利用该字典进行探测。

- 字典内容：可添加用户名与密码，格式为“用户名：密码”，中间用冒号（：）分割，每条字典记录独立一行。用户名和密码不能包含冒号。
- 字典上传：选择密码库上传，格式与字典内容格式相同，扩展名为 dic 文件
- 【导入字典】：点击导入，字典文件上传。
- 【导出字典文件】：点击链接下载字典内容
- 【保存】：点击【保存】按钮，保存添加的字典内容。
- 【恢复默认字典】：恢复最初始的字典。

远程协助字典

远程协助字典中包含使用远程连接时可能经常使用的用户名及密码，弱密码扫描利用该字典进行探测。

- 字典内容：可添加用户名与密码，格式为“用户名：密码”，中间用冒号（：）分割，每条字典记录独立一行。用户名和密码不能包含冒号。
- 字典上传：选择密码库上传，格式与字典内容格式相同，扩展名为 dic 文件
- 【导入字典】：点击导入，字典文件上传。
- 【导出字典文件】：点击链接下载字典内容
- 【保存】：点击【保存】按钮，保存添加的字典内容。
- 【恢复默认字典】：恢复最初始的字典。

SMB 字典

SMB 字典中包含使用 SMB 共享时可能经常使用的用户名及密码，弱密码扫描利用该字典进行探测。

- 字典内容：可添加用户名与密码，格式为“用户名：密码”，中间用冒号（：）分割，每条字典记录独立一行。用户名和密码不能包含冒号。
- 字典上传：选择密码库上传，格式与字典内容格式相同，扩展名为 dic 文件
- 【导入字典】：点击导入，字典文件上传。
- 【导出字典文件】：点击链接下载字典内容
- 【保存】：点击【保存】按钮，保存添加的字典内容。
- 【恢复默认字典】：恢复最初始的字典。

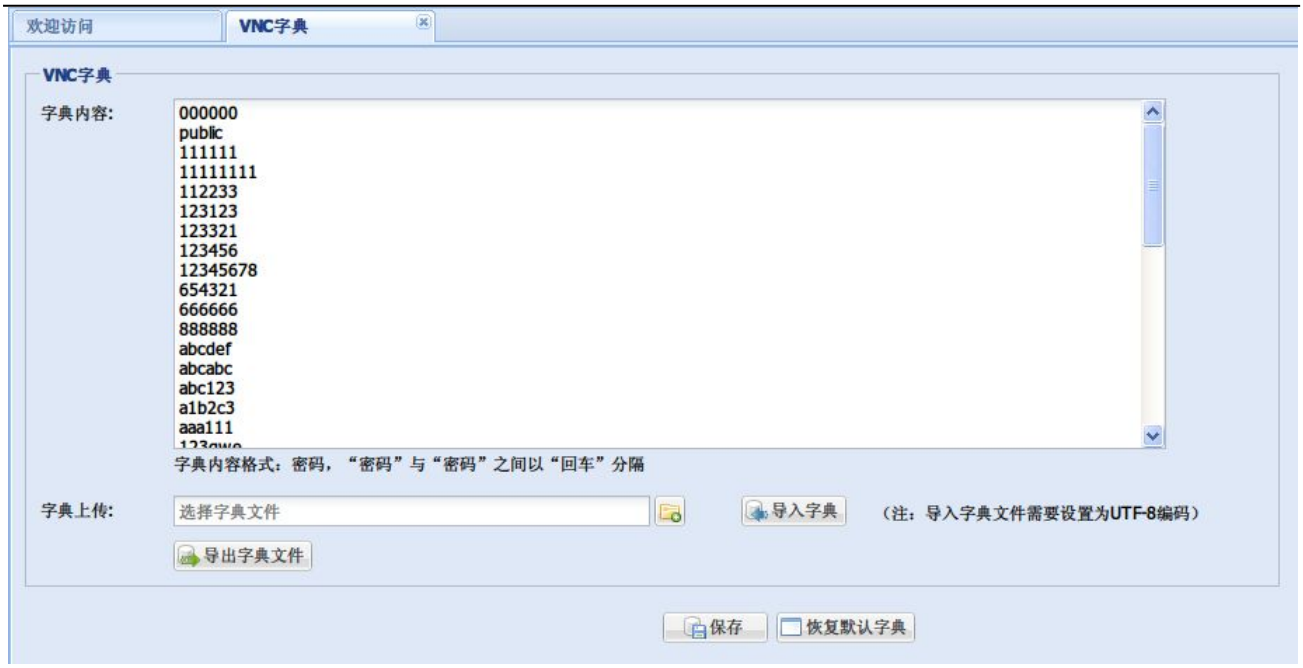
SSH 字典

SSH 字典中包含使用 SSH 时可能经常使用的用户名及密码，弱密码扫描利用该字典进行探测。

- 字典内容：可添加用户名与密码，格式为“用户名：密码”，中间用冒号（：）分割，每条字典记录独立一行。用户名和密码不能包含冒号。
- 字典上传：选择密码库上传，格式与字典内容格式相同，扩展名为 dic 文件
- 【导入字典】：点击导入，字典文件上传。
- 【导出字典文件】：点击链接下载字典内容
- 【保存】：点击【保存】按钮，保存添加的字典内容。
- 【恢复默认字典】：恢复最初始的字典。

VNC 字典

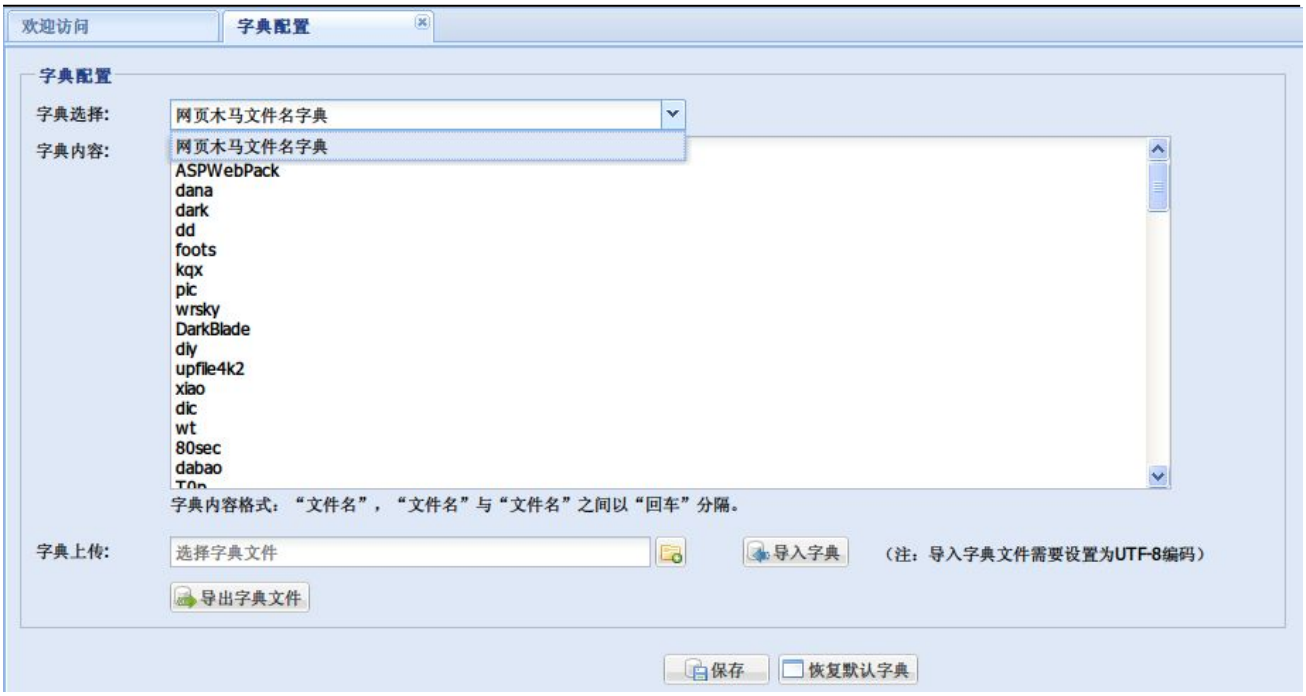
VNC 字典中包含使用 VNC 时可能经常使用的密码，弱密码扫描利用该字典进行探测。



- 字典内容：可添加密码，格式为“密码”，“密码”与“密码”之间以“回车”分隔。
- 字典上传：选择密码库上传，格式与字典内容格式相同，扩展名为 dic 文件
- 【导入字典】：点击导入，字典文件上传。
- 【导出字典文件】：点击链接下载字典内容。
- 【保存】：点击【保存】按钮，保存添加的字典内容。
- 【恢复默认字典】：恢复最初始的字典。

网页木马文件名字典

网页木马文件名字典中包含网页木马常用的文件名，WEB 漏洞扫描利用该字典进行探测，判断是否含有网页木马。



- 字典内容：可添加文件名，格式为“文件名”，“文件名”与“文件名”之间以“回车”分隔。
- 字典上传：选择密码库上传，格式与字典内容格式相同，扩展名为 dic 文件。
- 【导入字典】：点击导入，字典文件上传。
- 【导出字典文件】：点击链接下载字典内容。
- 【保存】：点击【保存】按钮，保存添加的字典内容。
- 【恢复默认字典】：恢复最初始的字典。

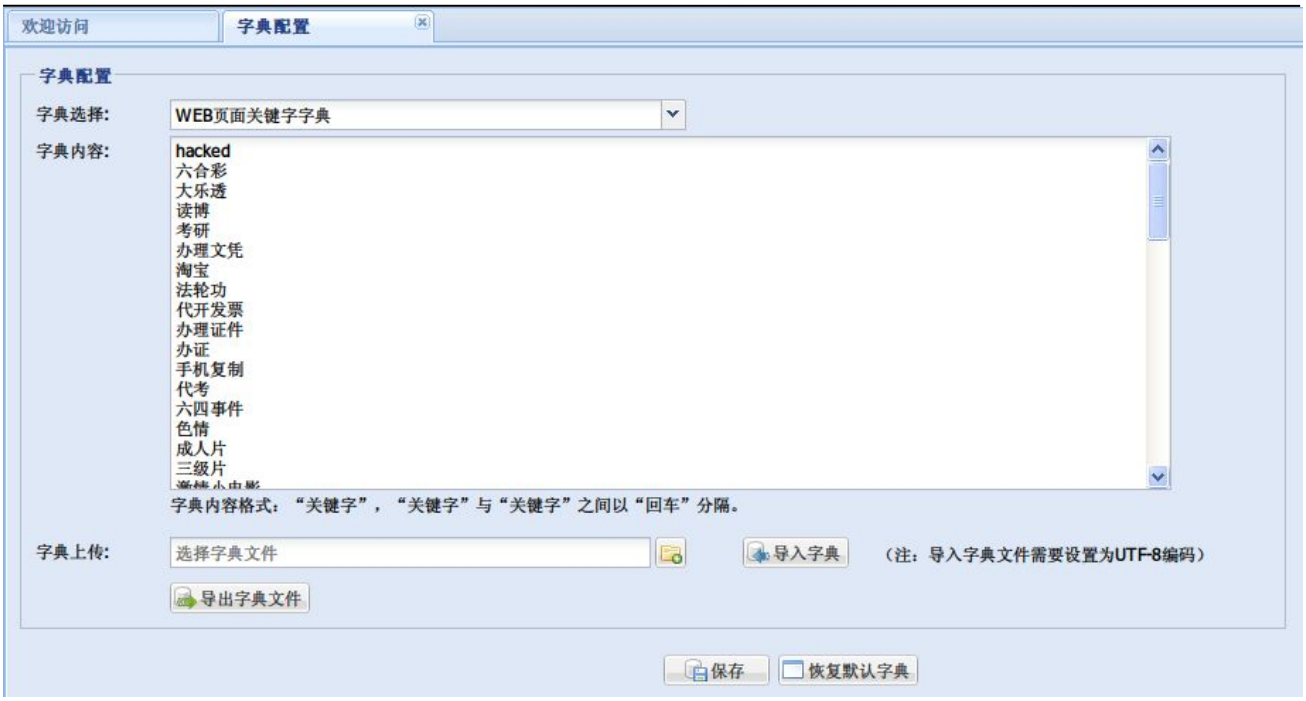
WEB 弱密码字典

WEB 弱密码字典中包含 Web 登录页面经常使用的表单弱密码，WEB 漏洞扫描利用该字典进行探测。

- 字典内容：可添加用户名与密码，格式为“用户名：密码”，中间用冒号（：）分割，每条字典记录独立一行。用户名和密码不能包含冒号。
- 字典上传：选择密码库上传，格式与字典内容格式相同，扩展名为 dic 文件
- 【导入字典】：点击导入，字典文件上传。
- 【导出字典文件】：点击链接下载字典内容。
- 【保存】：点击【保存】按钮，保存添加的字典内容。
- 【恢复默认字典】：恢复最初始的字典。

WEB 页面关键字字典

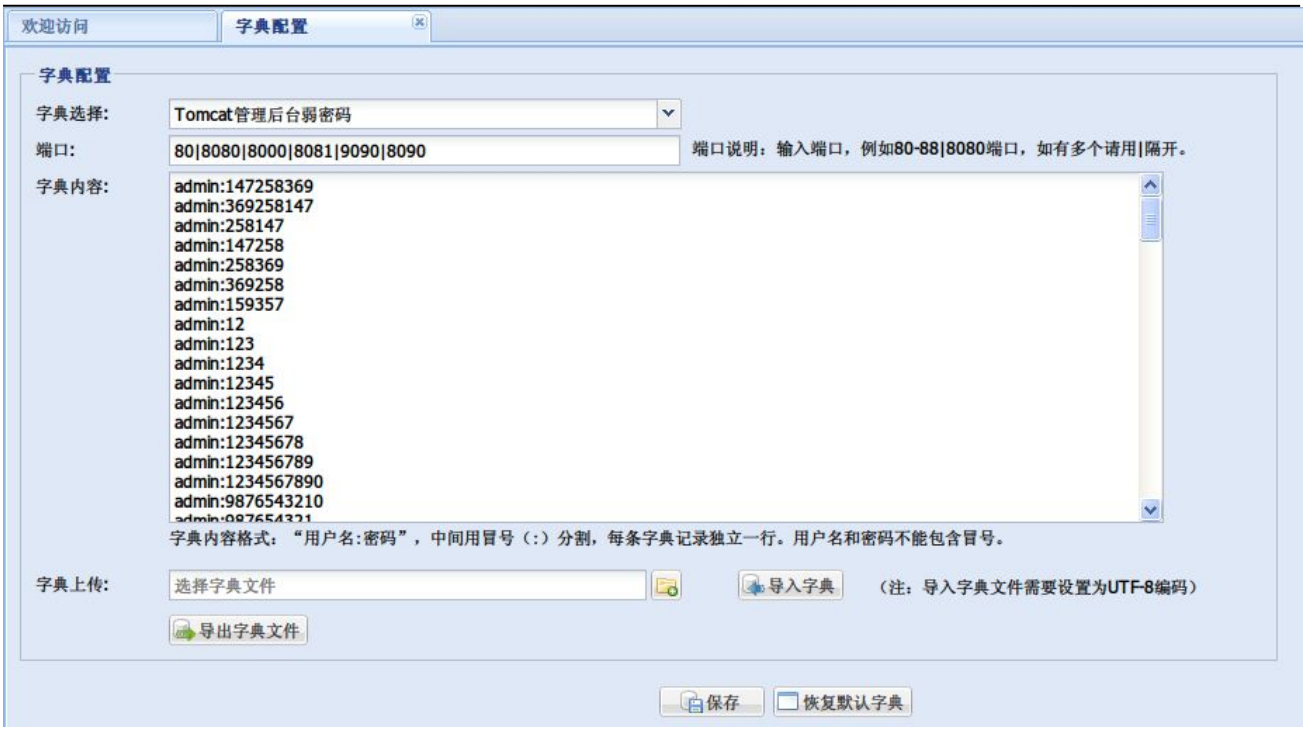
WEB 页面关键字字典中包含 Web 页面常用的非法关键字、暗链信息，WEB 漏洞扫描利用该字典进行探测。



- 字典内容：可添加用户名与密码，格式为“用户名：密码”，中间用冒号（：）分割，每条字典记录独立一行。用户名和密码不能包含冒号。
- 字典上传：选择密码库上传，格式与字典内容格式相同，扩展名为 dic 文件
- 【导入字典】：点击导入，字典文件上传。
- 【导出字典文件】：点击链接下载字典内容。
- 【保存】：点击【保存】按钮，保存添加的字典内容。
- 【恢复默认字典】：恢复最初始的字典。

Tomcat 管理后台弱密码

Tomcat 管理后台弱密码中包含 Tomcat 后台登录常用的弱密码，WEB 漏洞扫描利用该字典进行探测。



- 字典内容：可添加用户名与密码，格式为“用户名：密码”，中间用冒号（：）分割，每条字典记录独立一行。用户名和密码不能包含冒号。
- 字典上传：选择密码库上传，格式与字典内容格式相同，扩展名为 dic 文件
- 【导入字典】：点击导入，字典文件上传。
- 【导出字典文件】：点击链接下载字典内容。
- 【保存】：点击【保存】按钮，保存添加的字典内容。
- 【恢复默认字典】：恢复最初始的字典。

⚠注意：

1. **用户名和密码中不能包含“：”（冒号）；**
2. **导入字典文件的格式需要设置为 UTF-8 编码。**

用户设置

用户设置（系统管理员适用）

系统管理员可在“用户设置”页面中添加、修改和删除用户。系统管理员可以在此页面修改自己的密码。

- 添加用户： 具有系统管理员权限的用户可以添加安全管理员账号和普通用户账号，点击【添加】按钮弹出如图的对话框，输入相关信息后点击【保存】按钮即添加一个用户。

提示：

默认最大扫描任务数为 10，为所有用户一共所能执行的任务数，添加用户时超过最大扫描任务时，将保存失败；修改扫描任务数时，可不用填写用户密码直接修改并保存即可。

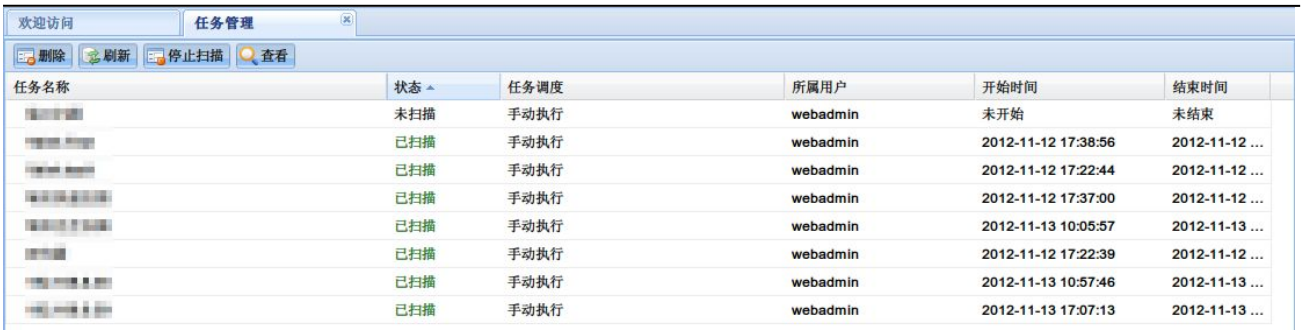
- 修改用户： 修改选定的用户，例如修改用户密码或者权限类型。
- 删除用户： 删除选定的用户。
- 查询用户： 在右侧输入用户名后点击【快速查询】按钮，系统将符合条件的用户在【用户设置】页面显示出来。
- 设置：对密码强度和登录次数进行设置，如图。

口令长度为至少 10 位，口令长度范围为（10～32），密码强度至少为数字和字母的组合。

登录的次数的设定，默认值是 3，也是最大值，用户可以根据自己的需求设定。此功能是针对同一用户，在登录次数超过设定值时，锁定该用户，在 15 分钟内不允许用户登录，15 分钟后自动解除锁定该用户。

任务管理（系统管理员适用）

系统管理员可在“任务管理”页面中删除、停止扫描任务。



- 【删除】： 选择需要删除的任务，点击【删除】按钮，成功删除任务。
- 【停止扫描】： 选择需要停止的任务，点击【停止扫描】按钮，成功停止扫描。
- 【查看】： 选择需要查看的任务，点击【查看】按钮，可以查看扫描任务的参数设置。

用户设置（安全审计员适用）

安全审计员可在“用户设置”页面中添加、修改和删除用户。安全审计员可以在此页面修改自己的密码。

- 添加用户： 具有安全审计员权限的用户可以添加安全审计员，点击【添加】按钮弹出如图的对话框，输入相关信息后点击【保存】按钮即添加一个用户。

- 修改用户： 修改选定的用户，例如修改用户密码。
- 删除用户： 删除选定的用户。
- 查询用户： 在右侧输入用户名后点击【快速查询】按钮，系统将符合条件的用户在【用户设置】页面显示出来。

14、系统

固件升级

通过固件升级，您可以获得最新的产品功能或者加固的产品安全性能。请联系铱迅信息客服人员，然后提交产品序列号，根据您所购买的产品型号获取相应的固件升级文件，在本页面选择升级文件后，点击【升级】按钮，完成产品升级。升级后，请进入【系统日志】页面查看相关系统日志。

规则升级

通过规则升级，您可以获得最新的产品漏洞规则库。请联系铱迅信息客服人员，然后提交产品序列号，根据您所购买的产品型号获取相应的规则升级文件，在本页面选择升级文件后，点击【升级】按钮，完成产品规则升级。升级后，请进入【系统日志】页面查看相关系统日志。

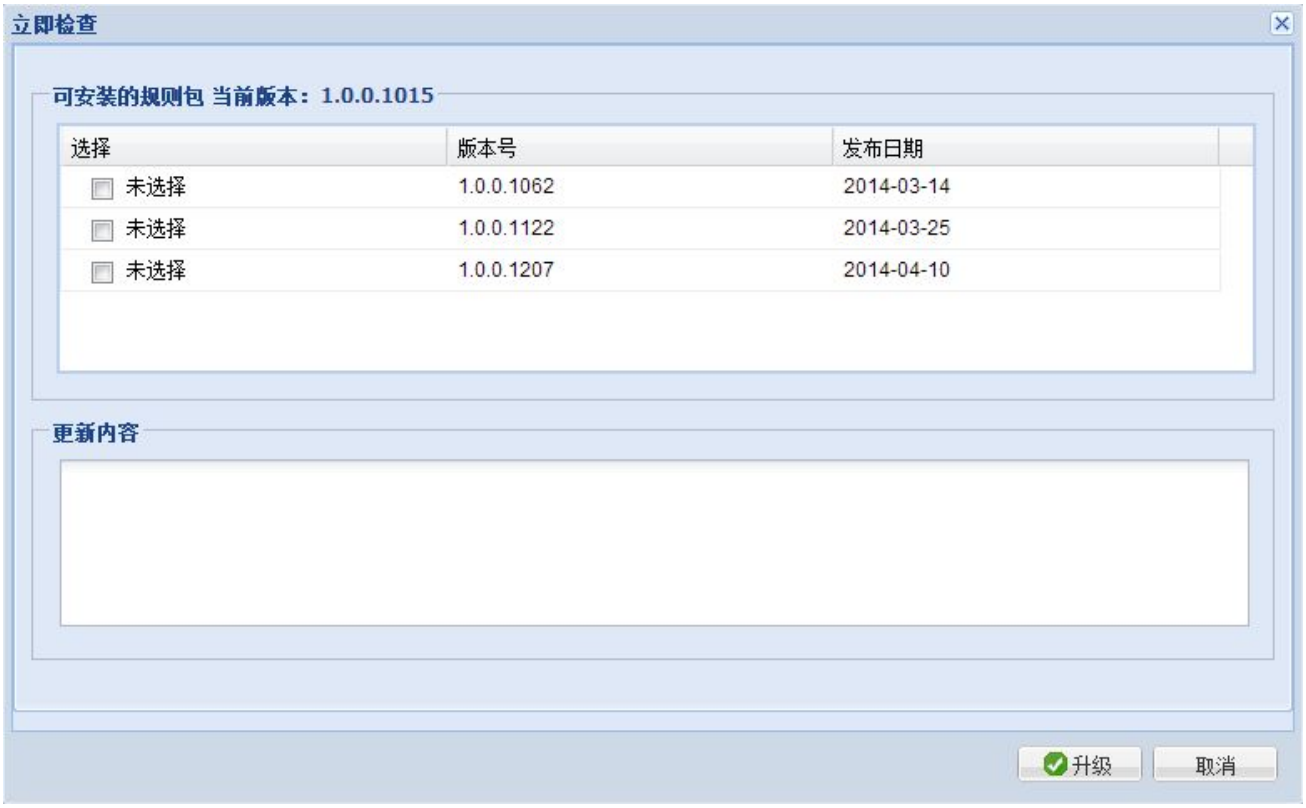
在线升级

通过在线升级，您可以实时获取最新的固件升级包和规则升级包。在连接网络的情况下，从在线升级服务器（http://yxupdate.yxlink.com）上下载最新的固件升级包和规则升级包，通过手动升级或自动升级以确保铱迅漏洞扫描系统的固件和规则处于最新状态。升级后，请进入【系统日志】和【在线升级日志】页面查看相关系统日志。

进入漏洞扫描系统后，点击功能菜单【系统】-【在线升级】，设置在线升级配置。

- 升级类型：设置升级的类型，分为固件升级和规则升级；
- 升级来源：设置在线升级服务器，默认在线升级服务器为：http://yxupdate.yxlink.com；
- 升级方式：设置升级方式，分为三种
  1) 自动升级到最新版本：设置为当前升级方式后，当在线升级服务器出现最新升级包时，则会下载升级包并升级。
  2) 不自动升级，有更新时提醒我：设置为当前升级方式后，当在线升级服务器出现最新升级包时，则在每次登录设备会出现悬浮框进行提醒：“系统提示 系统检测到有最新升级包，固件升级包版本：*.*.*.*;规则升级包版本：*.*.*.*”。同样，可以点击功能菜单【状态】-【系统状态】的许可证及设备信息一栏中，也可以查看到最新固件版本和最新规则版本的提示。
  3) 关闭自动升级：设置为当前升级方式后，则系统不会自动升级。
- 升级周期：升级方式设置为自动升级后，可设置升级周期为每天、每周或每月的某个时段自动去检查并升级。
- 是否启动 HTTP 代理：提供 HTTP 代理去连接在线升级服务器，可设置代理站点、端口、用户名和密码。

- 保存：以上配置设置完成，点击【保存】按钮保存当前页面相关配置；若当前升级方式为固件升级，则保存的相关配置只与固件升级有关；反之，当前升级方式为规则升级，则保存的相关配置只与规则升级有关。
- 立即检查：点击【立即检查】按钮，弹出“立即检查”页面。该页面可显示最新可安装的固件包和规则包，可选择进行手动升级。



注意：

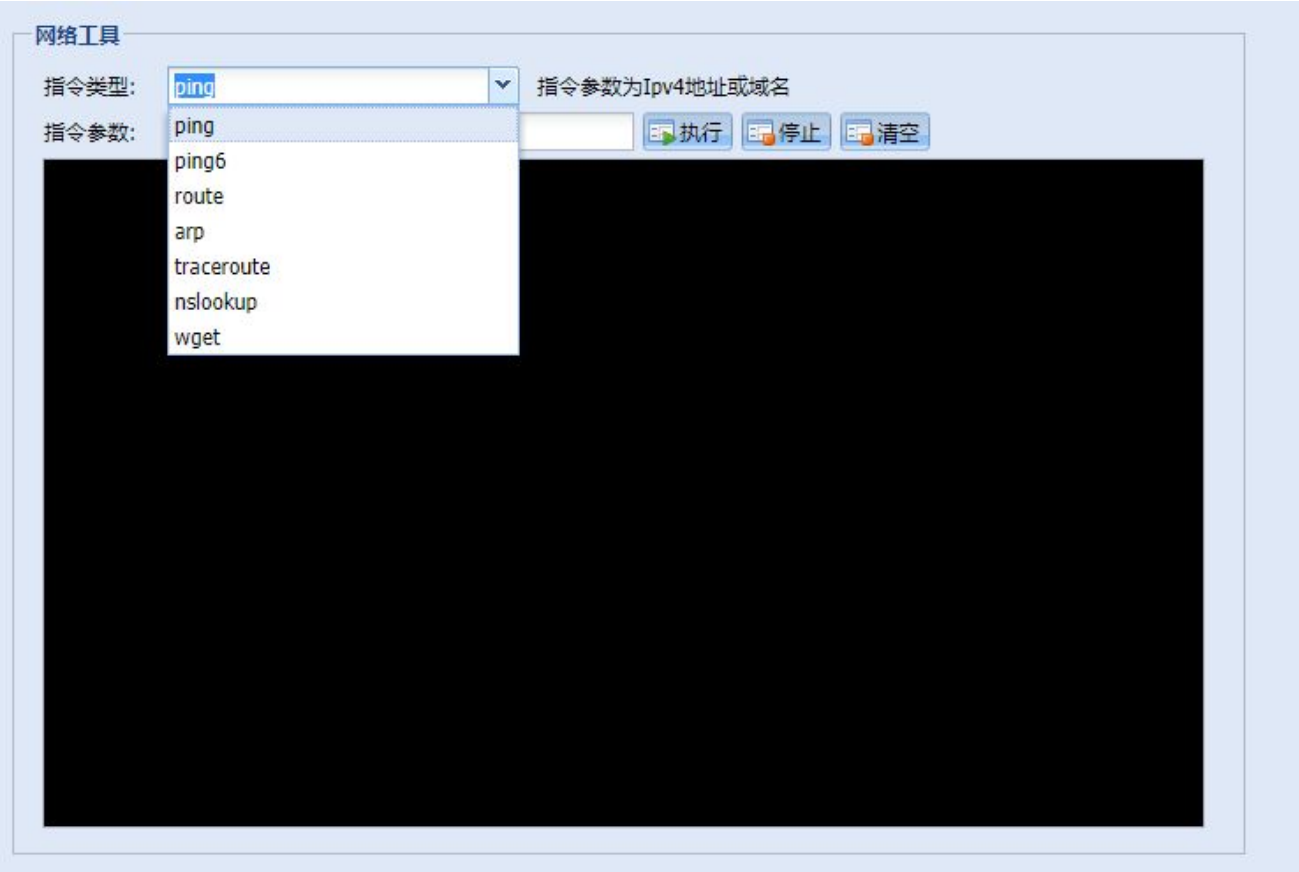
如果漏洞扫描系统的系统版本在 3.0.03.4028 之前，请先联系铱迅信息客服人员获取固件升级包和规则升级包以及相关的功能授权。手动进行固件升级和规则升级，优先升级固件升级包（此次升级时间较长，中途切勿关机或重启）；

系统配置

本页面设置设备的系统时间。设置好时间后，点击【应用】按钮，完成系统时间设定。

网络工具

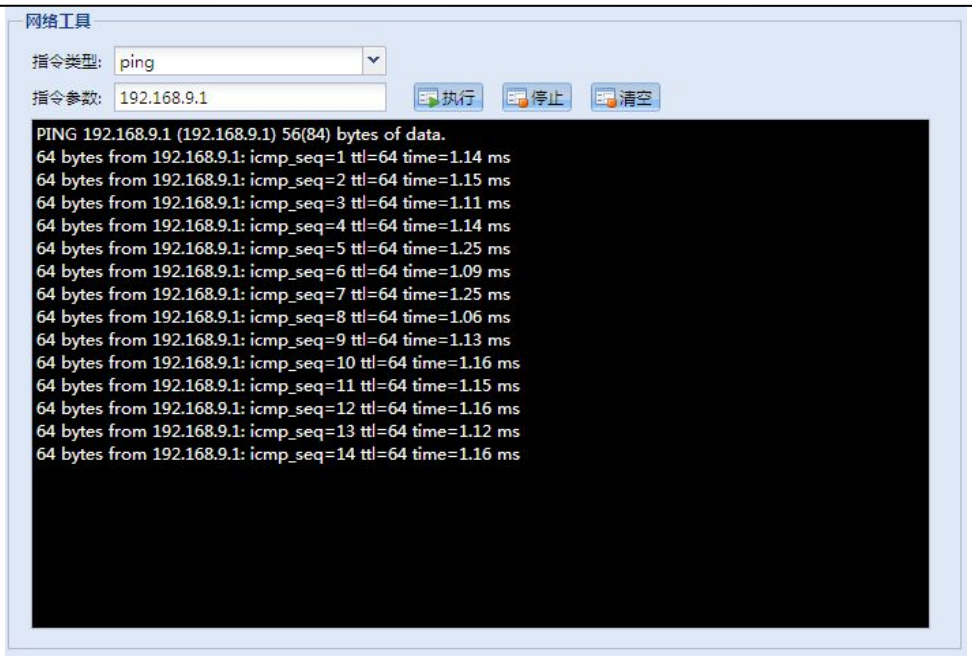
本设备内部添加的一个包含有 ping、route、arp、traceroute 和 nslookup 的网络工具。



- 指令类型：点击下拉框，可以选择 7 条常用指令中的一条。
- 指令参数：相应指令所对应的参数，比如 ping 指令可以设定参数为域名或 IP 地址。
- 执行：执行选择的操作指令。
- 停止：一些操作指令需要手动停止，比如 ping。
- 清空：清除界面上显示的信息。

使用 ping 指令：可以检测本设备的网络连接状况

选择指令类型为 ping，指令参数设定为 192.168.9.1，点击执行，出现如下信息。其他指令您可以参照 windows 下命令行的相对应指令信息使用。



重新启动

本页面用于对设备进行“关机”与“重启”操作。

- 关机： 点击【关机】按钮，稍后将会安全关闭设备。
- 重启： 点击【重启】按钮，将会重新启动设备。

⚠注意：

1. 请您尽量避免在本设备正常运行的时候直接切断电源。

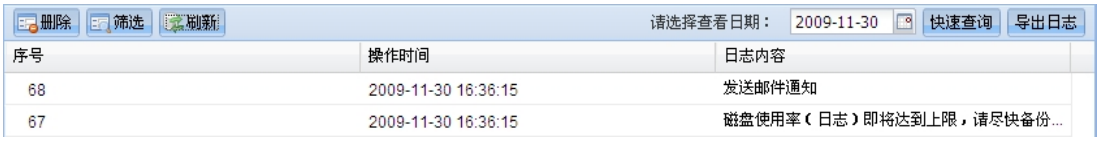
（这样可能造成数据的丢失或者影响设备的使用寿命）

2. 在您点击【关机】按钮，或者直接按下本设备上的电源按钮后，请等待电源指示灯熄灭后再切断电源，设备安全关闭需要一定时间。

15、日志

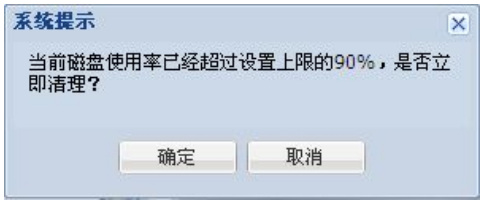
系统在磁盘日志空间使用率将满或者已满的情况下，系统有三种提示用户的方式。

1、记录到系统日志，如下图：

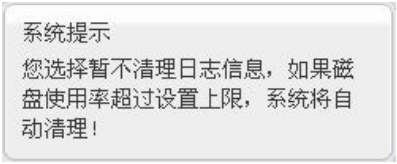


2、邮件通知：如果用户使用了通知设置，在日志将满或者已满时，会收到相关邮件。

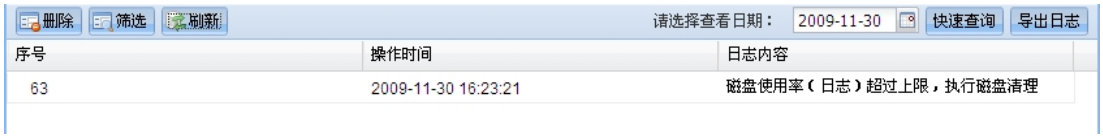
3、登录提示：在安全管理员登录时，系统自动弹出一个提示对话框，如图：



若点击“确定”按钮，则自动跳转到“磁盘日志清理”页面，具体请参考 18.3.2 手动磁盘清理。若点击“取消”按钮，不做清理，就会出现一个系统提示，如图：

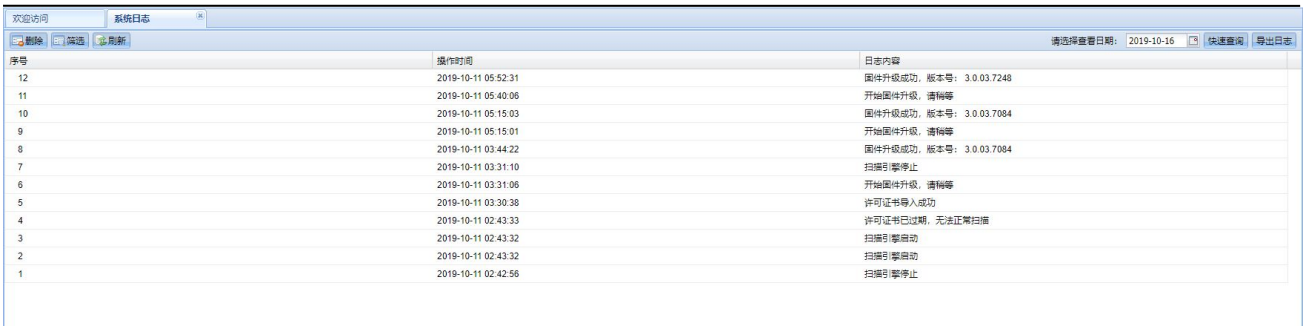


系统在磁盘空间使用率已满的情况下，自动做磁盘清理操作，自动磁盘清理日志会记录到系统日志当中，如图所示：

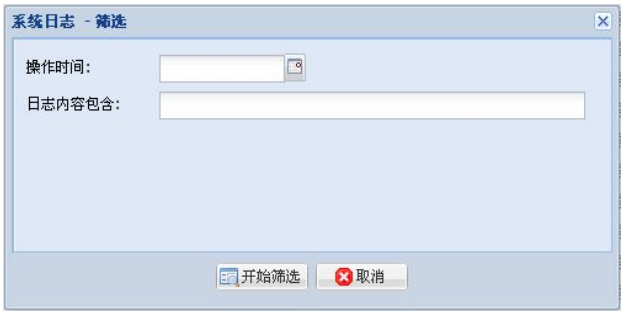


系统日志

系统日志页面显示了本设备上的系统事件，如图，您可以通过查询日志了解本设备上所发生的所有系统事件。



- 系统事件查询： 在右上侧选择或者输入指定日期，点击【快速查询】按钮，可以查询指定日期的系统日志。
- 导出日志： 选择某个日期，点击【导出日志】按钮，导出指定日期的日志信息，以 csv 文件形式保存，您可以选择用 Microsoft Excel 等工具查看导出的系统日志文件。
- 日志筛选：点击【筛选】按钮，弹出【系统日志-筛选】对话框，如图。您可以组合日期和日志包含内容条件，筛选出需要查看的系统日志。



- 取消筛选：点击【取消筛选】按钮，可以取消已经筛选出的日志列表，恢复到正常状态。
- 删除日志：选择一条或者多条系统日志，点击【删除】按钮，这些系统日志将被从系统中删除。

⚠注意：

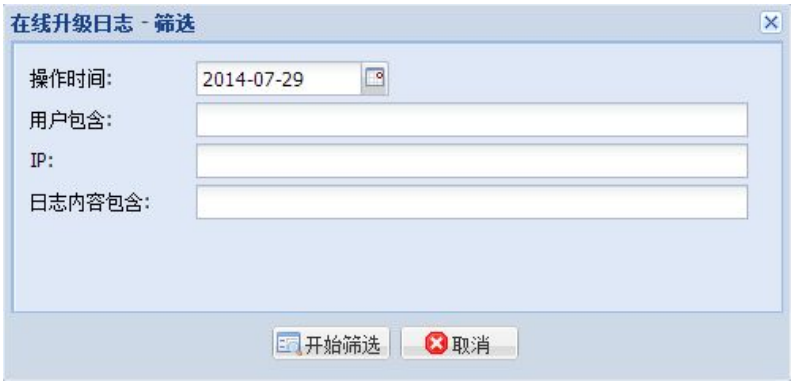
系统会根据当前的磁盘空间上限设置，自动定期执行日志清理工作。如果需要保留日志，请参见 18.3 磁盘日志清理。

在线升级日志

在线升级日志用于记录在线升级时的升级信息。

- 在线升级日志查询： 在右侧选择或者输入指定日期，点击【快速查询】按钮，可查询指定日期的在线升级日志。

- 导出日志： 选择某个日期，点击【导出日志】按钮，导出当天的日志信息，以 csv 文件形式保存，您可以选择用 Microsoft Excel 等工具查看导出的审计日志文件。
- 日志筛选：通过筛选功能，可以快速筛选出需要查看的在线升级日志。点击【筛选】按钮，弹出【在线升级日志-筛选】对话框，如图。您可以组合日期和日志包含内容条件，筛选出需要查看的日志。



- 取消筛选：点击【取消筛选】按钮，可以取消已经筛选出的日志列表，恢复到正常状态。

审计日志(安全审计员适用)

审计日志用于安全审计员审查设备的使用情况，用户对设备配置所作的修改操作都将被记录到审计日志中。

- 审计日志查询： 在右侧选择或者输入指定日期，点击【快速查询】按钮，可查询指定日期的审计日志。

- 导出日志： 选择某个日期，点击【导出日志】按钮，导出当天的日志信息，以 csv 文件形式保存，您可以选择用 Microsoft Excel 等工具查看导出的审计日志文件。
- 日志筛选：通过筛选功能，可以快速筛选出需要查看的审计日志。点击【筛选】按钮，弹出【审计日志-筛选】对话框，如图。您可以组合日期和日志包含内容条件，筛选出需要查看的日志。

- 取消筛选：点击【取消筛选】按钮，可以取消已经筛选出的日志列表，恢复到正常状态。

磁盘日志清理

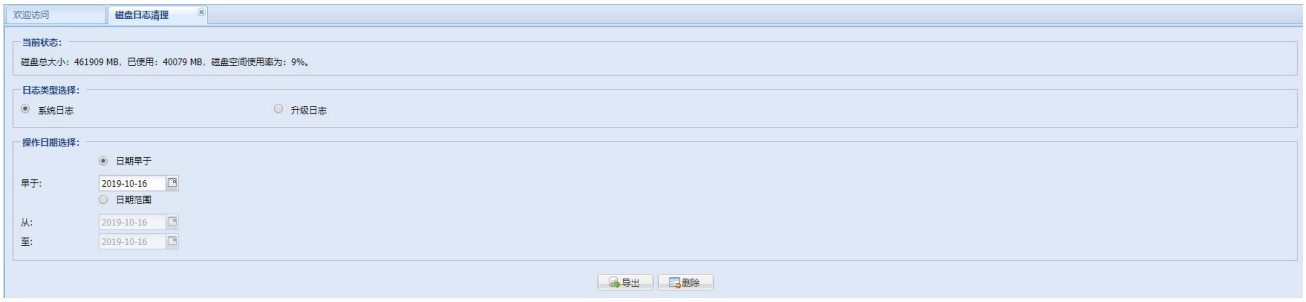
系统运行会产生各种日志信息，但过多的日志信息会影响系统的正常运行，建议用户定期对磁盘中的日志进行清理。

自动磁盘清理

系统会在磁盘空间使用率达到设置上限时自动执行磁盘清理工作。设备的“自动清理”会从最早的日志记录开始清理，直到磁盘空间的使用率低于设置值，所以请您记得定期备份日志。

手动磁盘清理

除了系统自动清理功能，您还可以手动进行磁盘清理，在手动清理时，建议您先将日志导出后再删除。



- 当前状态： 显示磁盘当前的使用情况，用户可根据磁盘使用率来决定是否进行清理。
- 日志类型选择： 选择要处理的日志类型。
- 操作日期选择： 可选择某个日期之前的所有记录或者选择一个日期的范围。
- 导出日志： 首先选择需要导出的日志类型和时间范围，点击【导出】按钮，导出的格式为 csv 文件。请用 Microsoft Excel 等软件查看。导出的日志将无法再导入到设备中。

- 删除日志： 首先选择需要删除的日志类型和时间范围，点击【删除】按钮，则指定的日志被直接删除。

⚠注意：

日志删除后不可以恢复，请您确认不再需要查看所选的日志后再决定将其删除。建议您在删除前将日志导出以便日后查看。

16、Console 功能

Console 口可以对设备进行常用配置，特别是当设备无法通过 Web 方式进行正常的管理维护的时候，可以通过 Console 功能，对设备进行管理，查看设备的状态，对设备进行配置、复位或还原等操作。

- 登录：用 PC 连接设备 Console 口，输入用户名：conadmin　密码：conadmin。

```
**************************************************************************
*                                                                        *
*       Welcome to Yxlink Network Vulnerability Scan System              *
*                    You can input ? for help                            *
*                                                                        *
**************************************************************************
NVS>>
```

- 帮助：输入“？”或者“help”。

主菜单

在主菜单界面输入“?”显示”主菜单目录”，主菜单提供常用的网络命令 ping，route，traceroute，nslookup，查看设备信息以及关机重启等操作。

```
NVS>>
configure                Enter configure model
show                     Show all information
arp                      Display Arp table
ping                     Send echo messages
route                    Display the IP routing table
traceroute               Trace route to destination
nslookup                 Query Internet name servers
reboot                   Reboot the system
shutdown                 Shutdown the system
help                     List all available commands
exit                     Quit the console
NVS>>
```

主菜单常用命令

显示接口信息：

NVS>> show interface

显示设备信息：

NVS>> show nvsinfo

显示网卡 MAC 地址：

NVS>> show macaddress

显示 ARP 信息：

NVS>> arp

重启：

NVS>> reboot

关机：

NVS>> shutdown

配置菜单（configure）

在主菜单输入： *configure* 进入*配置*菜单，在*配置*主菜单界面输入“？”显示*配置*菜单目录，*配置*菜单可以配置 DMI，DSI，DNS，DHCP，还原，复位等操作。

```
NVS(configure)#
system                          Set the system information
show                            Display some configuration
restore                         Restore the software
reset                           Reset the device
help                            List all available commands
exit                            Exit from configure mode
```

配置菜单常用命令

参数说明：

netmask 子网掩码

gateway 网关

ip_begin DHCP 起始 IP

ip_end DHCP 结束 IP

配置 DMI：

NVS(configure)#system interface DMI ip 192.168.9.10 netmask 255.255.255.0 gateway 192.168.9.1

配置 DSI：

NVS(configure)#system interface DMI ip 192.168.100.2 netmask 255.255.255.0 gateway 192.168.100.1

配置系统时间：

NVS(configure)#system clock 2012-09-12

配置首选 DNS：

NVS(configure)#system dns1 8.8.8.8

配置备用 DNS：

NVS(configure)#system dns2 9.9.9.9

配置 DHCP：

NVS(configure)#system dchp ip_begin 192.168.9.10 ip_end 192.168.9.100

修改密码：

NVS(configure)#system passwd 123456789

显示系统时间：

NVS(configure)#show clock

显示 DMI：

NVS(configure)#show DMI

显示 DSI：

NVS(configure)#show DSI

显示 DHCP：

NVS(configure)#show dhcp

显示 DNS：

NVS(configure)#show dns

还原：

NVS(configure)#restore

复位：

NVS(configure)#reset

返回上级菜单：

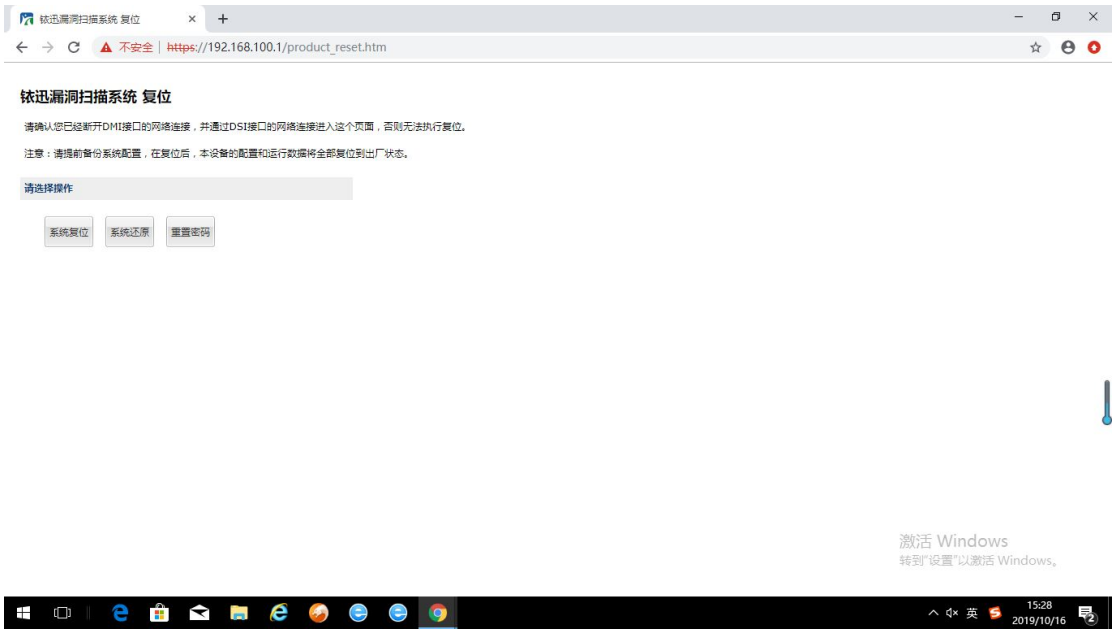
NVS(configure)#exit

⚠注意：

所有的参数请根据实际情况输入。

17、复位与还原

如需对设备复位，必须先断开 DMI 接口的网络连接，并通过 DSI 接口连接本设备。然后通过浏览器访问页面 https://192.168.100.1/product_reset.htm。此处的 192.168.100.1 可能根据您的具体设备有所不同，请参考附录 A.1. 设备设置接口(DSI 接口)初始设置。



点击【系统复位】将会使本设备的所有设置恢复到出厂值，所有的入侵记录和页面统计数据等日志数据将被清空，用户账户和密码将恢复到出厂值。

点击【系统还原】后，除了执行【系统复位】的操作外，还将会使设备固件恢复到出厂版本。只有在固件升级失败和系统异常时才可以使用。

点击【重置密码】后，系统的密码会恢复到默认初始密码。

⚠注意：

请提前备份系统配置并且导出重要的日志数据。在设备复位或还原后，本设备的配置和运行数据将全部恢复到出厂状态。

18、常见问题与解答

问题 1：如何知道本系统处于正常工作状态?

解答：可以添加一个可以正常访问的网站，点击扫描，查看扫描状态是否正常。

问题 2：修改某个设置后，好像没有生效?

解答： 请点击该页面的【应用】按钮后等待 1 分钟左右，设置生效需要一定时间。

问题 3：如何正常关闭设备?

解答：按下本设备背面的电源按钮或者进入【重新启动】页面后点击【关机】按钮。安全关闭设备需要一定时间，前面板的 Power 灯熄灭后，设备正常关闭。

问题 4：无法进入 Web 管理页面怎么办?

解答：

（1）请先确认计算机能和本设备进行正常通讯（如果计算机开启了防火墙，请将 443 端口打开）。

（2）如果仍然无法进入 Web 管理页面，请尝试从 DSI 接口连接。

（3）开机状态下，通过 USB 键盘输入“resetnvs”进行手动复位。

问题 5：忘记管理员密码怎么办?

解答： 可以通过复位密码重置管理员密码。首先，拔下 DMI 接口的网线，从 DSI 接口用网线连接计算机，并参考《铱迅漏洞扫描系统安装部署手册》设置您的计算机网络参数。在浏览器中访问 https://192.168.100.1/product_reset.htm，根据提示进行产品密码重置。

问题 6：固件升级失败怎么办?

解答：如果升级失败，请首先检查设备是否工作正常。如果一切正常，请忽略此失败事件。如果不正常，请参考问题 5 进行产品复位。如果仍然无法解决此问题，请联系铱迅客服人员。

附录 A. 出厂默认设置

A.1. 设备设置接口(DSI 接口)初始设置

IP 地址	192.168.100.1
子网掩码	255.255.255.0

A.2. 预置账号

A.2.1. 系统管理员预置账号

用户名	sysadmin
密　码	sysadmin

A.2.2. 安全审计员预置账号

用户名	auditor
密　码	auditor

A.2.3. 安全管理员预置账号

用户名	webadmin
密　码	webadmin

A.2.4. Console 用户预置帐号

用户名	conadmin
密　码	conadmin

A.3. 默认设置

设置项	配值
远程文件包含的 URL 配置	远程文件包含的 URL：http://www.yxlink.com/nvs_test.txt 包含关键字：vulnerability test
域名检测端口配置	80|81|8000|8080|8088|8090

铱迅信息（YXLink）

南京铱迅信息技术股份有限公司

江苏省南京市雨花台区宁双路 18 号沁恒科技园 D 幢 4 层

Nanjing YXLink Information Technology Co.,Ltd.