BEYOND
TECHNOLOGY

NSAM：
东软NetEye安全评估与监控系统产品快速向导

Neusoft

目 录

前言

文档范围

本文详细介绍东软 NetEye 安全评估与监控系统（简称 NSAM）的 Web 管理界面和串口管理界面的快速配置向导，适用于 V2.0 软件版本。

期望读者

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

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

获得帮助

如需获取网络安全相关资料，请

访问网站：http://neteye.neusoft.com/

咨询热线：400-6556789

许可证管理

许可证是版权拥有者对产品使用者行为的一种约束和规定，一般定义了用户使用该产品的条件。许可证绑定了产品的硬件信息。如果许可证所绑定信息与当前使用的硬件信息不匹配，则该许可证是不合法的，不可被使用。许可证由厂家统一制作，只有当系统被上载许可证之后，用户才能对产品进行配置。许可证管理在系统管理员 account 下操作。

许可证使用步骤如下：

1）导出许可证

登录系统管理员账号，选择“License 管理”，点击“导出许可证”，导出 reqlic 文件。如下图 2-1-1 示：

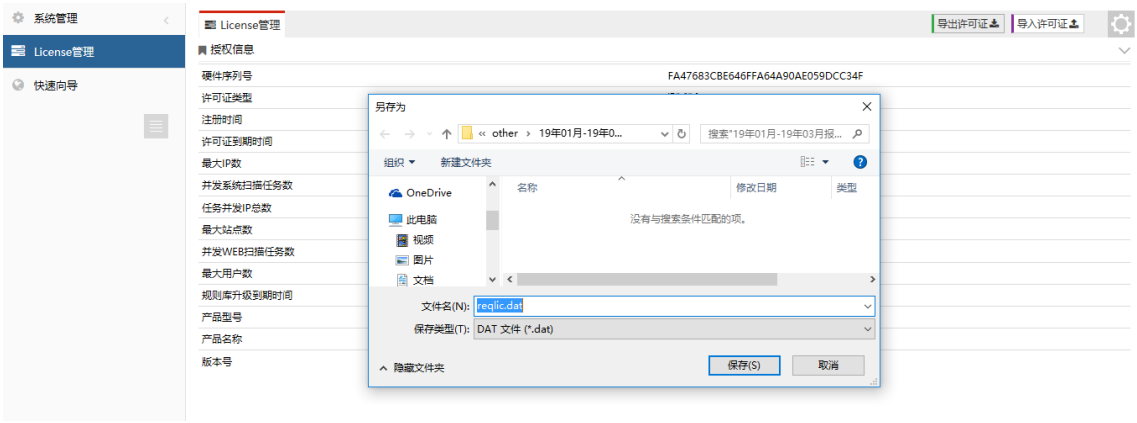

图 2-1-1 导出许可证

2）制作许可证

该步骤由厂商完成，随每个产品附带许可文件。

3）导入许可证

登录系统管理员账号，选择“License 管理”，点击“导入许可证”，导入制作好的.dat 授权文件。如下图 2-1-2 所示：

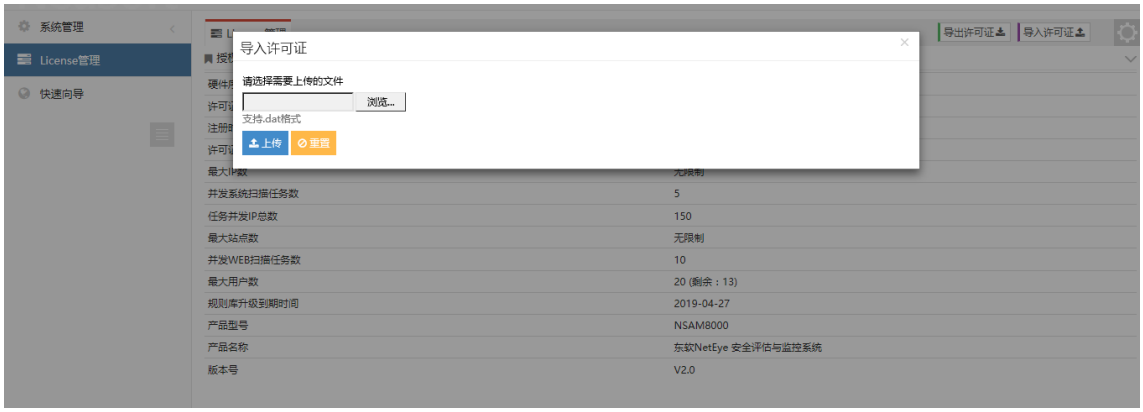

图 2-1-2 导入许可证

4）查看许可证

在“License 管理”下查看许可的类型、时间、型号等信息，如下图 2-1-3 所示：

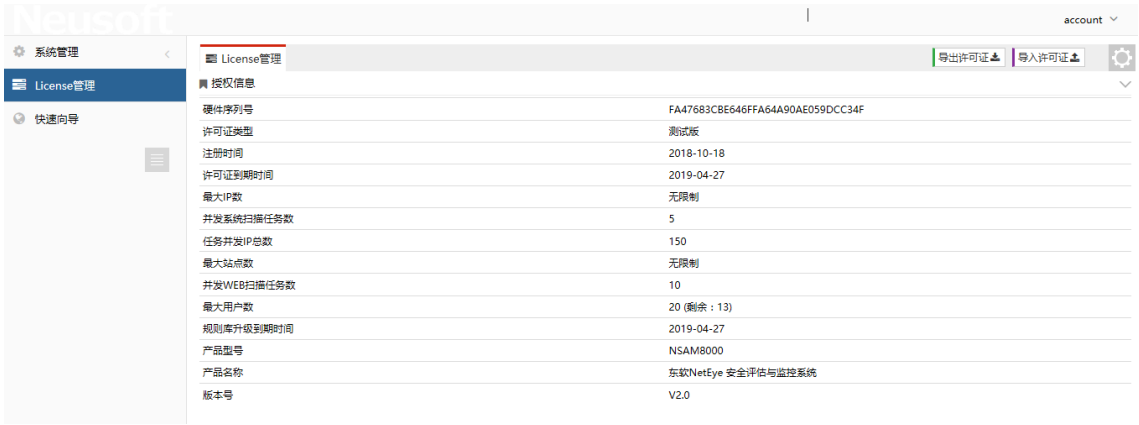

图 2-1-3 查看导出许可证

1.概述

该文档将引导您如何把东软 NetEye 安全评估与监控系统（NSAM）快速安装到您的网络里。但是每个网络的环境、需求、安全策略等均存在差异，NSAM 的配置也会有所不同。该文档仅以典型的实例进行说明，如需更详细的配置请咨询 Neusoft 客服中心。

2.部署前准备

※详细了解网络拓扑、需进行漏洞扫描的资产所在位置

※确定 NSAM 的部署位置

※了解网络中防火墙等安全设备位置，并开放 NSAM 对资产的访问权限

※准备一台 PC、一根交叉线

※将 NSAM 从包装箱中取出，并检查相关配件是否齐全

3.NSAM 出厂默认参数

※WAF 网口初始设置

接口	eth0 ---eth5
IP	192.168.1.100
网络掩码	255.255.255.0

※WEB 配置管理方式

注：需使用 IE7 以上浏览器（需支持 AJAX），建议使用火狐浏览器

管理方式	https://192.168.1.100
系统管理员	admin/admin
帐号管理员	account/account
审计管理员	audit/audit

※串口管理方式

串口通讯参数	
波特率	9600
传输位数	8
奇偶校验	无
停止位	1
数据流控制	无
串口管理员	
串口管理员	admin/aDmin@3.21

4.管理登录 NSAM

※将 NSAM 上电，开机运行

※ PC 用交叉线连接 NSAM 的任意网口

※把 PC 的 IP 改为 192.168.1.X

※在 PC 上打开浏览器（建议使用火狐），访问 https://192.168.1.100

※在出现证书安全提示时选择“是”（IE7 以上选择“继续访问”，firefox 则选择“我已充分了解可能的风险”并“添加例外”）

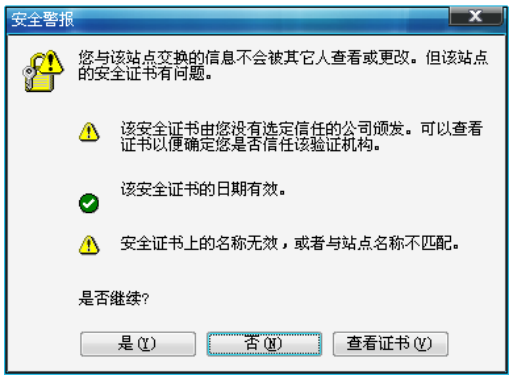

图 4-1 安全证警报

※在登录窗口中输入管理员的用户：account　密码: account

图 4-2 登录界面

※点登录后即可进入 NSAM 账户管理界面

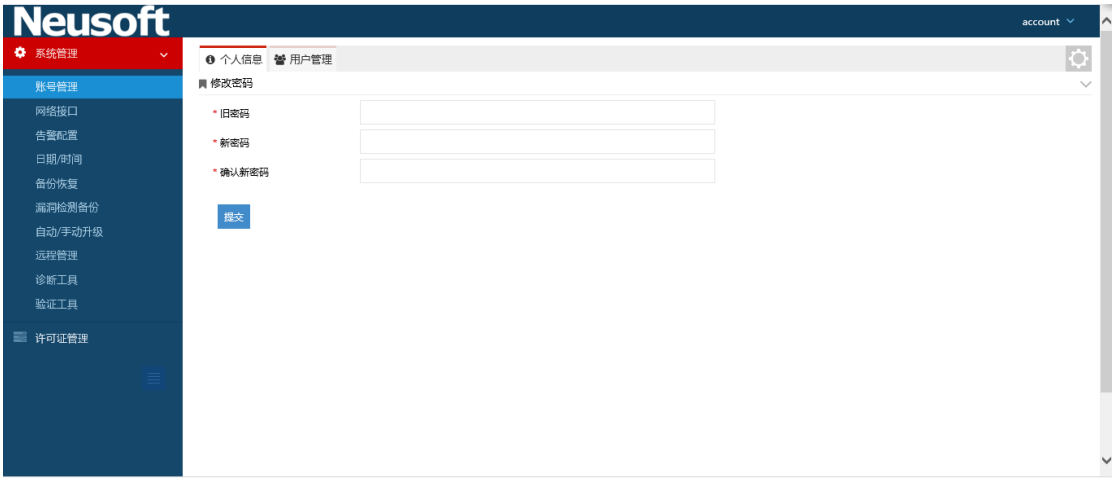

图 4-3 账户管理界面

5.基本配置

5.1 添加及修改 ip

※【系统管理】-->【网络接口】-->【ip 配置】，点击“新增”，如下图所示：

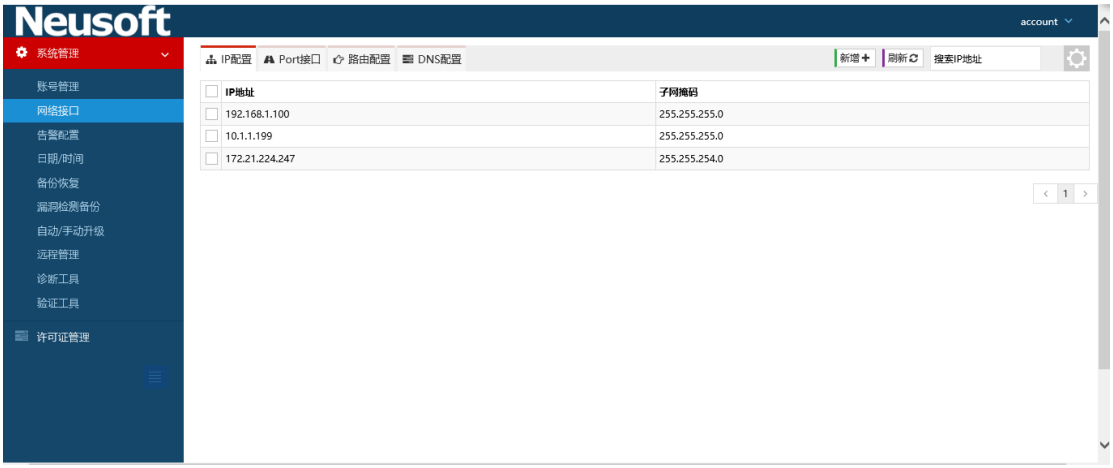

图 5-1-1 网络接口

※输入具体 IP 地址及子网掩码

图 5-1-2 ip 地址配置

※在路由配置下配置网关默认路由

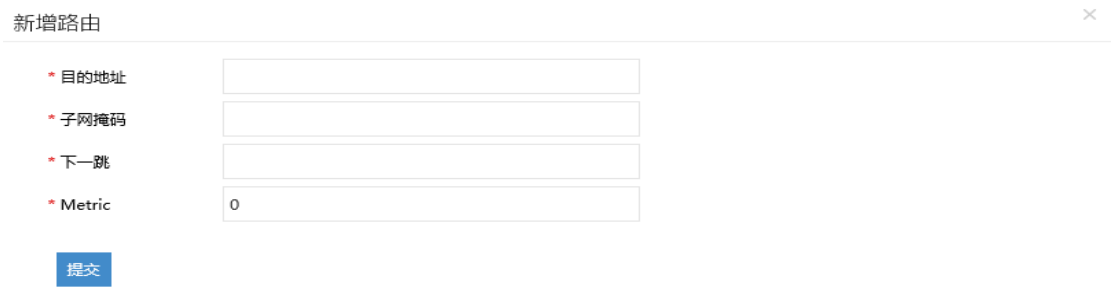

图 5-1-3 网关配置

6.设备应用配置

使用系统管理账户“admin”登录设备，在系统管理账户下完成对设备应用的配置。

6.1 新建扫描任务

6.1.1 扫描基本配置

【任务中心】-->【新建任务】，选择相应的扫描选项（系统扫描、WEB 扫描、安全基线扫描、数据库扫描），针对漏洞扫描，添加需要扫描的目标，填写形式为单个主机或者主机组，配

置任务名称，选择漏洞扫描插件模板并提交扫描。

图 6-1-1 新建任务

6.1.2 自主选择插件配置

可对扫描任务使用的插件进行修改，使用“启用”或者“禁用”在漏洞插件的基础上来增删漏洞插件，实现插件库自定义。

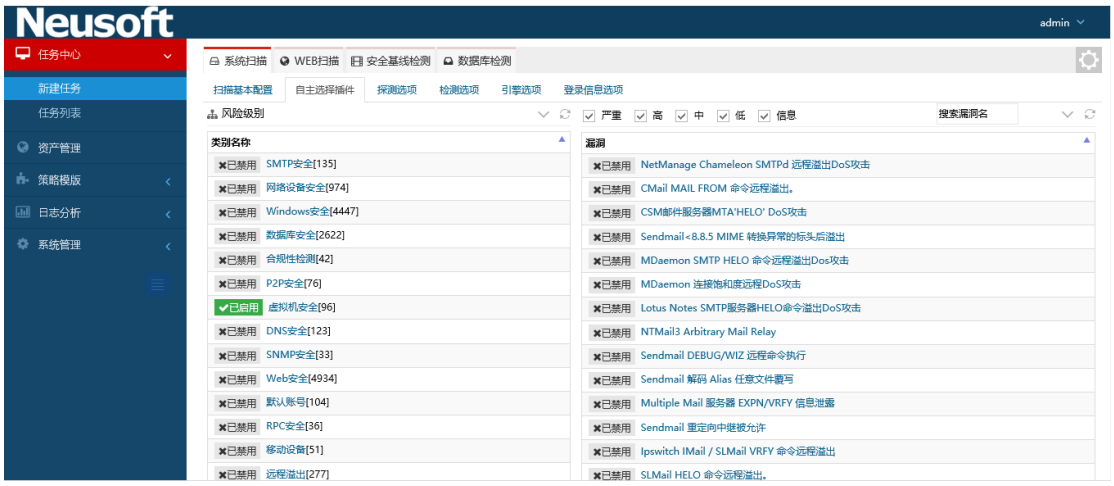

图 6-1-2 自主选择插件

6.2 任务列表

任务列表模块列出了目前存在的全部扫描任务，并可对任务扫描任务进行各种操作管理。方便用户开启任务和查看每个资产组的主机数，进度栏可显示扫描出的漏洞数，进度栏模块可以查看每个主机的检测进度、历史执行记录和漏洞风险分布情况。

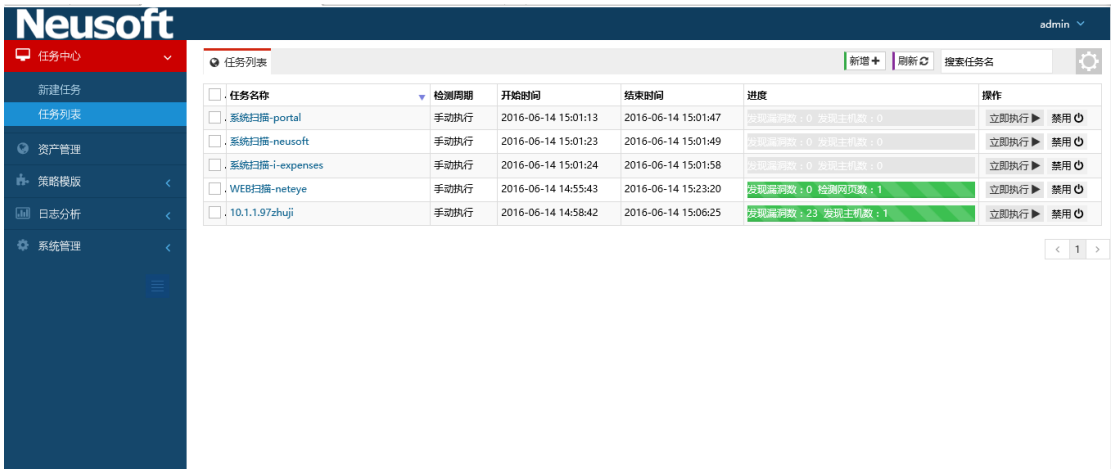

图 6-2 任务列表

6.3 策略模板

策略模板是基于脚本的规则库，包括系统插件和 web 插件，提供给用户可选的规则有 6 万多条，覆盖了 CVE、CNVD、CNNVD、CNCVE 等多个漏洞库中的所有漏洞。扫描器将定期发布最新的规则库，用户可以通过代理商或者我们的网站获得最新的规则库。

6.3.1 系统插件

系统内置全面的漏扫扫描插件，可以灵活的定义扫描扫描策略。

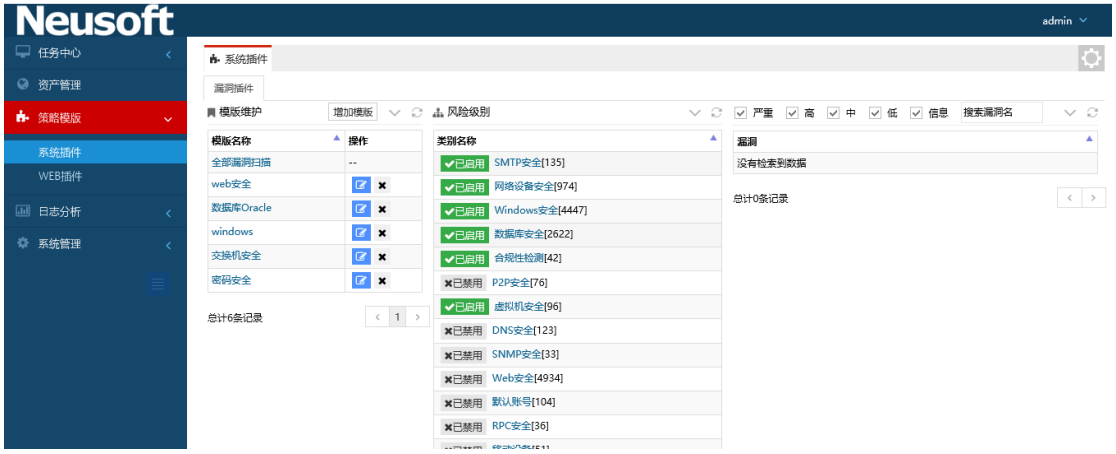

图 6-3-1 系统插件

6.3.2WEB 插件

预置的 web 漏洞插件库，包含当前最新的检测规则，提供全面的安全扫描策略，并能灵活定义扫描策略。

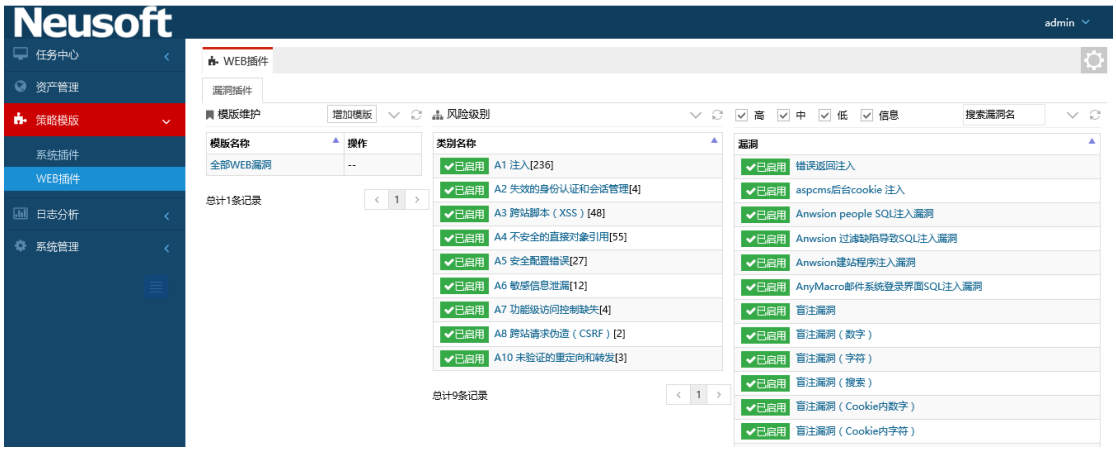

图 6-3-2WEB 插件

7.日志分析

7.1 在线查询

日志在线查询模块可以查看所有任务的扫描结果，包括扫描漏洞的详细信息和解决办法，同时可以根据需求只查询某个风险等级的漏洞。

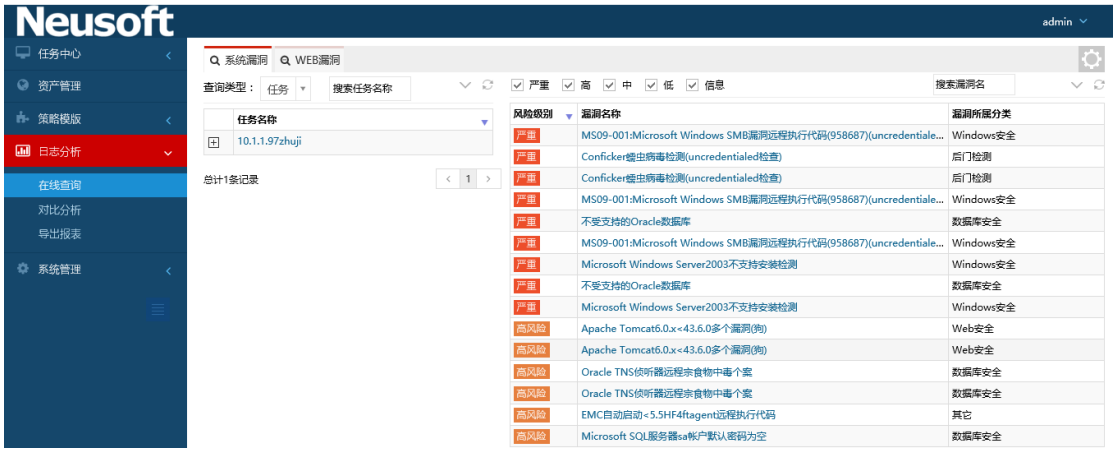

图 7-1 在线查询

7.2 对比分析

管理员可以选择多个任务点击对比分析对同一任务的多次扫描结果可任选两次进行对比分析，统计出新增和减少的漏洞以及漏洞变化趋势等。

图 7-2 对比分析

7.3 导出报表

可按照资产组和时间导出扫描报表，报表分为详细报告和统计报表，导出格式分为 HTML、WORD 和 EXCEL，报表标题可自定义。

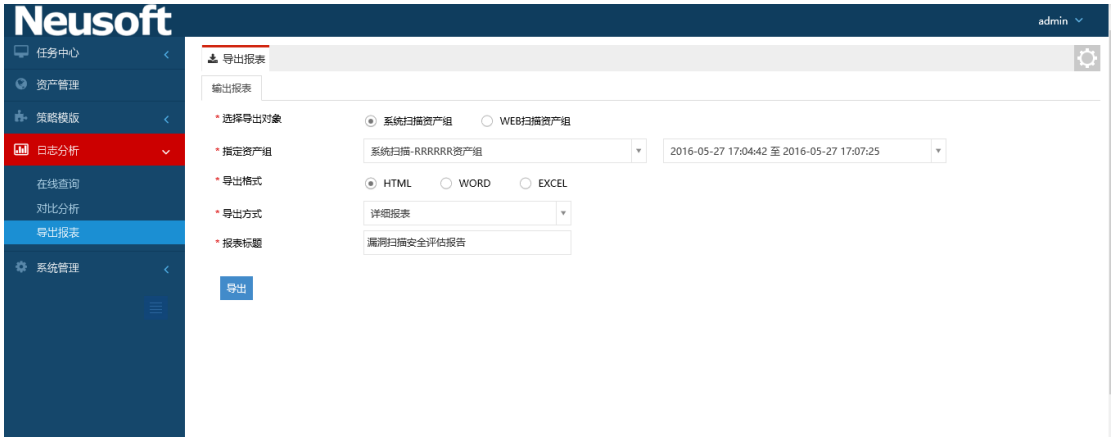
Neusoft
admin
任务中心
资产管理
策略模版
日志分析
在线查询
对比分析
导出报表
系统管理
导出报表
输出报表
* 选择导出对象
系统扫描资产组
WEB扫描资产组
* 指定资产组
系统扫描-RRRRRR资产组
2016-05-27 17:04:42 至 2016-05-27 17:07:25
* 导出格式
HTML
WORD
EXCEL
* 导出方式
详细报表
* 报表标题
漏洞扫描安全评估报告
导出

图 7-3 导出报表