UNIS XScan-G 系列漏洞扫描系统

Web 配置指导

目录

1 产品简介

1.1 产品概述

漏洞扫描系统是通过对系统漏洞、服务后门、网页挂马、SQL 注入漏洞以及跨站脚本等攻击手段多年的研究积累，总结出了智能主机服务发现、智能化爬虫和 SQL 注入状态检测等技术，可以通过智能遍历规则库和多种扫描选项组合的手段，深入准确的检测出系统和网站中存在的漏洞和弱点。最后根据扫描结果，提供测试用例来辅助验证漏洞的准确性，同时提供整改方法和建议，帮助管理员修补漏洞，全面提升整体安全性。

漏洞扫描系统以综合的漏洞规则库（本地漏洞库、ActiveX 库、网页木马库、网站代码审计规则库等）为基础，采用深度主机服务探测、Web 智能化爬虫、SQL 注入状态检测、主机配置检查以及弱口令检查等方式相结合的技术，实现了将 Web 漏洞扫描、系统漏洞扫描、数据库漏洞扫描与弱口令扫描于一体的综合漏洞评估系统。

1.2 登录介绍

设备已经设置了默认的 Web 登录信息，用户可以通过管理地址（初始默认地址 https://192.168.0.1），直接使用默认信息登录 Web 界面，首次登录会强制更改初始密码（建议使用 firefox 浏览器）。默认 Web 登录信息请参见表 1-1。

表1-1 漏洞扫描系统-分布式管理平台默认 Web 登录信息表

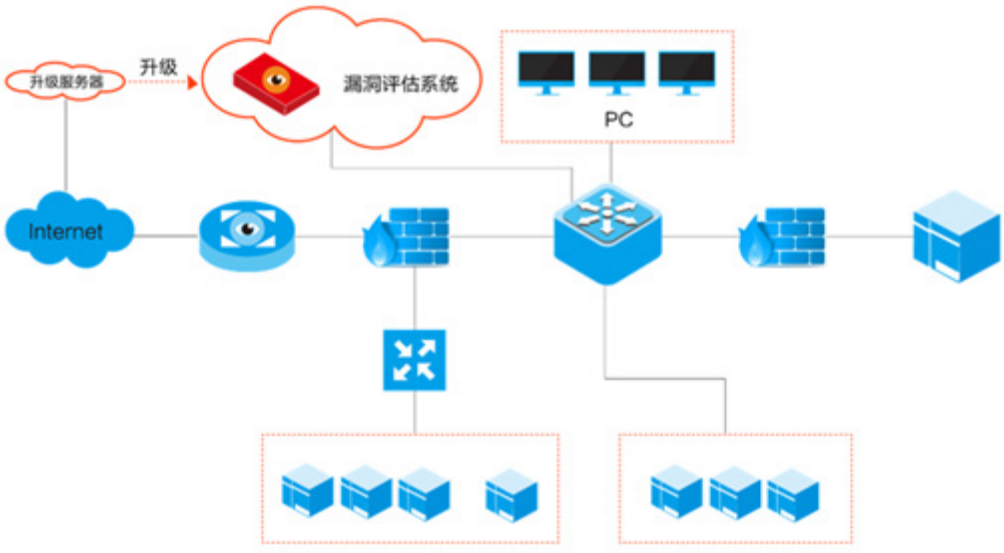
登录信息项	默认配置			
用户名	admin	account	audit	report
密码	admin	account	audit	report
描述	系统管理员	账户管理员	审计管理员	报表管理员

2 网络部署

2.1 拓扑示例

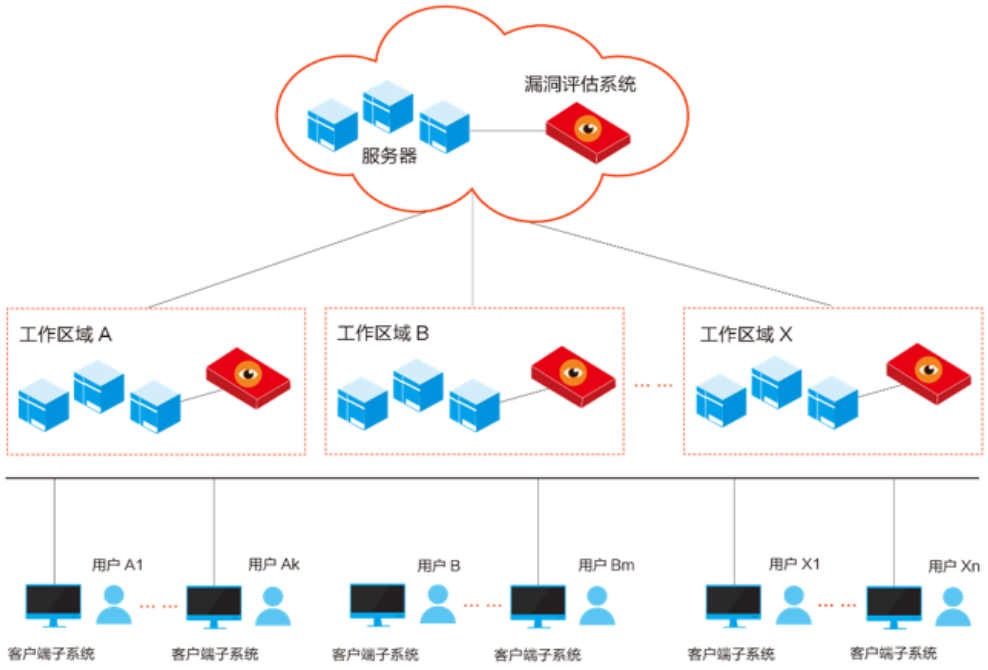
对于组网集中，网络规模较大但无绝对隔离限制的场景，可旁路部署在核心交换机上，对各个区域的设备进行扫描，单机部署操作简单，不改变客户现有网络结构。拓扑结构如下图。

图2-1 单机部署拓扑结构图



大型企业在全国各地都设有办公地，通常是大规模跨区域的网络，漏洞扫描产品部署在各个地区，在总部进行集中管理。漏洞扫描系统支持分布式部署，集中管控中心既可作为管理端，也可以作为扫描引擎，统一下发扫描任务至下级引擎，并在管控中心统一分析、统一展示。拓扑结构如下图。

图2-2 单机部署拓扑结构图



3 系统管理

本章介绍漏洞扫描系统提供的如下管理功能：

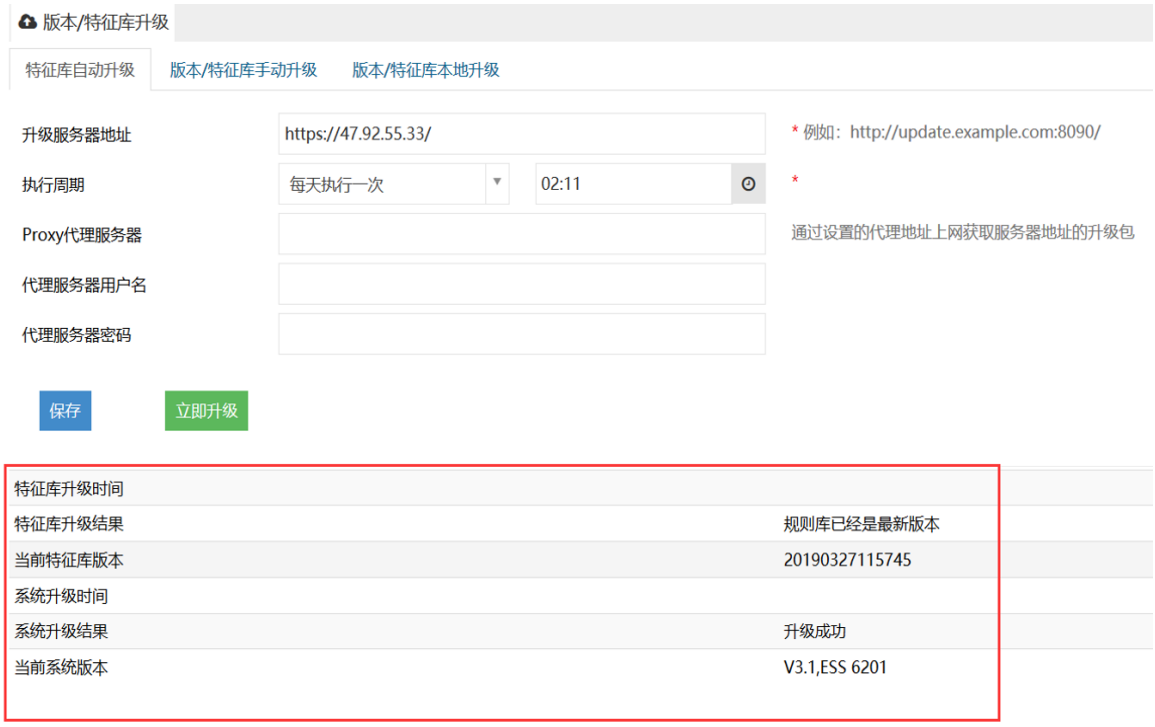
- 账号管理
- 网络配置
- 外发配置
- 告警配置
- 系统告警日志
- 分布式部署
- 日期时间
- 配置备份恢复
- 版本/特征库升级
- 信任 IP
- 诊断工具
- 验证工具
- SNMP 管理

3.1 系统信息

系统信息用于展示当前软件系统版本、规则特征库版本、系统时间、系统资源使用率，以及 syslog 配置、系统时间配置等信息。

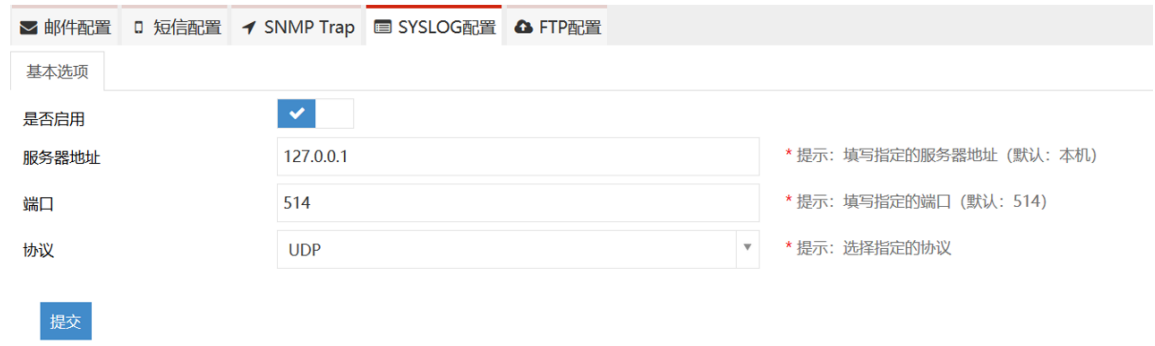
(1) 登录 account 账户，选择系统管理>版本/特征库升级,可以查看系统/规则特征库版本；

图3-1 系统/规则特征库版本信息



(2) 选择系统管理>外发配置>syslog 配置，可以查看或修改 syslog 配置信息；

图3-2 syslog 配置信息



(3) 选择系统管理>日期/时间，可以查看或修改系统时间配置信息。

图3-3 日期/时间

3.2 账号管理

本章介绍账户管理的相关内容。

3.2.1 账号管理

在主页面选择：系统管理>账号管理>账号管理

(1) 修改口令必须输入正确的旧密码，如果旧密码输入错误，则不允许修改，口令长度最少为 8 位；

(2) 修改口令成功后，将在下次登录时要求输入新的口令。

图3-4 修改密码

3.2.2 用户管理

(1) 系统设置了两个缺省用户：account 账户管理员和 admin 系统管理员。account 账户可以新建普通用户。在 account 账户配置网络。

(2) 用户可根据实际情况在 account 和 admin 上做用户管理；

(3) 所以账户的总和，无限制，包括系统管理员、账户管理员、审计管理员、报表管理员；

(4) 新创建的账户默认密码与账户名相同。

1. 新增用户

在主页面选择：系统管理>账号管理>用户管理

(1) 选择系统管理>用户管理>用户管理；

(2) 点击新增，添加新用户并配置新增用户信息如图 3-6。

图3-5 用户管理

图3-6 新增用户

表3-1 用户管理参数说明

参数	说明
用户名称	自定义用户名称
用户权限模板	不同的权限模板对应的功能模块各不相同
登录错误锁定	登录错误超过次数后，账户被锁
登录超时（分钟）	登录后无操作等待超时时间
限制系统扫描IP范围	该账户将无法扫描该IP
是否开启密码期限策略	密码的使用期限设置
是否开启密码强度策略	密码强度设置

3.2.3 用户锁定

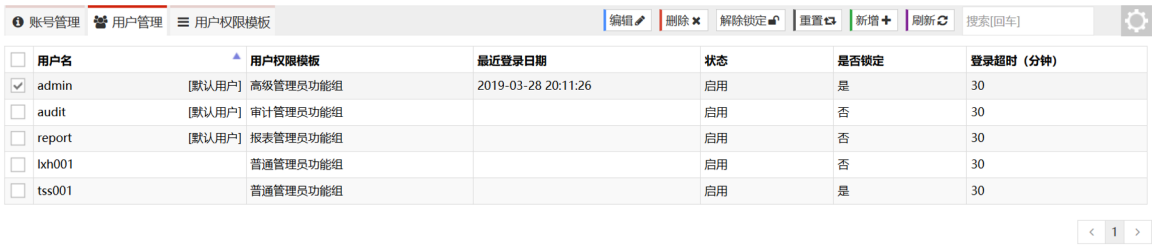
登录 account 账户，在主页面选择：系统管理>账号管理>用户管理

当账号被锁定时，登录 account 账户将锁定账号解除锁定。

(1) 选择系统管理>账号管理>用户管理；

(2) 点击被锁定用户>点击解除锁定。

图3-7 用户锁定列表



3.3 网络配置

在主页面选择：系统管理>网络接口

该功能用于配置漏洞扫描系统的网桥配置、路由配置、接口配置、DNS 配置。

(1) 选择系统管理>网络接口>IP 管理配置，进入网桥配置，默认有 MngtVlan，IP 地址为 192.168.0.1（管理地址），可在 MngtVlan 中新增 IP 地址，点击编辑，添加业务 IP。点击新增可添加网桥，点击 IP 管理可为新增网桥添加 IP 地址，每个网桥最多支持配置 8 个 IP 地址。点击删除可删除当前网桥。选择系统管理>配置备份恢复，点击备份可备份当前网络配置；勾选此备份可将当前网络配置备份下载或恢复；点击上传，可将之前下载备份的网络配置恢复。

图3-8 配置备份

图3-9 网桥配置

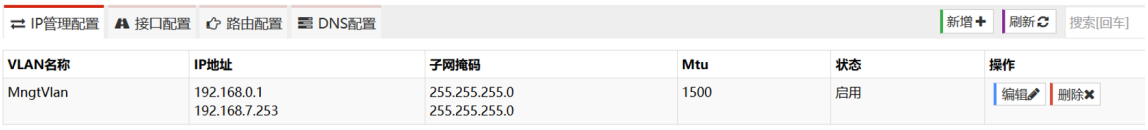


图3-10 IP 管理配置

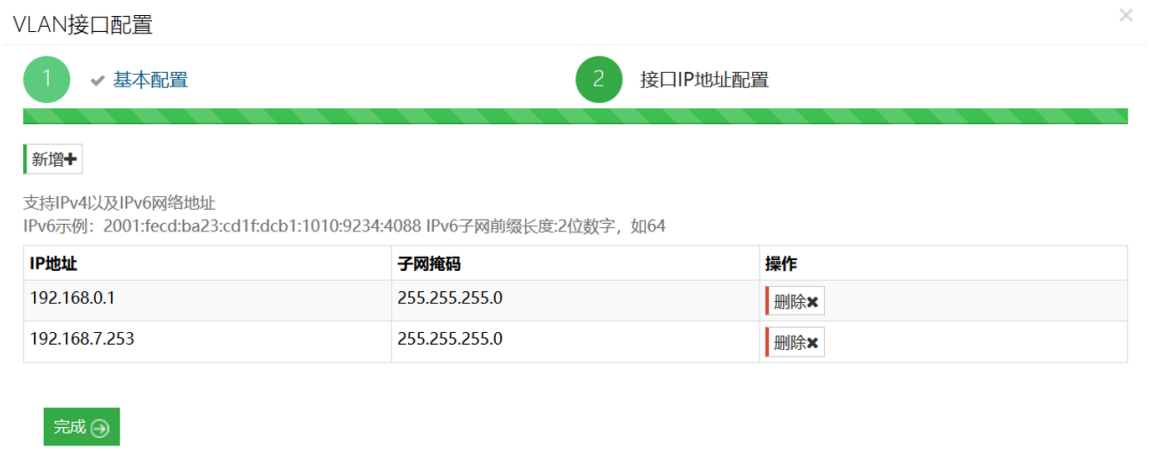


表3-2 网桥配置参数

参数	说明
网桥名称	网桥口的名称
IP/掩码	网桥的IP地址、掩码
状态	设置网桥接口的启用或禁用
操作	对网桥口做删除或编辑的操作

(2) 选择系统管理>网络接口>路由配置，进入路由配置界面，点击新增路由，添加相关路由配置。添加缺省静态路由，保证系统到被扫目标网络可达。

图3-11 路由配置

(3) 选择系统管理>网络接口>接口配置，进入接口配置界面，点击对应接口的编辑按钮，可配置当前接口所属网桥，以及物理状态是否开启。

图3-12 接口配置

接口名称	Vlan名称	接口启用/禁用	端口状态	发送速率(bps)	发包速率(pps)	接收速率(bps)	收包速率(pps)	操作
GE0/0	MngtVlan	启用	down	98	0	1	0	编辑
GE0/1	2	启用	up	0	0	0	0	编辑
GE0/2	MngtVlan	启用	down	0	0	0	0	编辑
GE0/3	MngtVlan	启用	down	0	0	0	0	编辑
GE0/4	MngtVlan	启用	down	0	0	0	0	编辑
GE0/5	MngtVlan	启用	down	0	0	0	0	编辑
GE1/0	MngtVlan	启用	down	0	0	0	0	编辑
GE1/1	MngtVlan	启用	down	0	0	0	0	编辑
GE1/2	MngtVlan	启用	down	0	0	0	0	编辑
GE1/3	MngtVlan	禁用	down	0	0	0	0	编辑
GE1/4	MngtVlan	启用	down	0	0	0	0	编辑
GE1/5	MngtVlan	启用	down	0	0	0	0	编辑
GE1/6	MngtVlan	启用	down	0	0	0	0	编辑
GE1/7	MngtVlan	启用	down	0	0	0	0	编辑

1

表3-3 接口配置参数

参数	说明
接口名称	管理界面显示的接口名称，如GE0/0
网桥名称	当前接口所处网桥
状态	设置接口的启用或禁用
端口状态	实际的物理接口的链路状态
发送速率	当前接口发送流量速率
发包速率	当前接口发包速率
接收速率	当前接口接收流量速率
收包速率	当前接口收包速率
操作	编辑当前接口所属网桥、启用或者禁用

(4) 选择系统管理>网络接口>DNS 配置，进入 DNS 配置界面，编辑主备 DNS 服务器地址。

图3-13 DNS 配置

表3-4 DNS 服务器说明

参数	说明
主DNS服务器	主用DNS服务器的IP地址，默认为8.8.8.8
备DNS服务器	备用DNS服务器的IP地址，默认为114.114.114.114

3.4 外发配置

3.4.1 邮件服务器配置

告警设置包括邮件告警与短信告警，本系统可以通过设置电子邮件进行邮件通知，在配置完成并保存以后可以通过发送测试邮件，确定配置的是否正确。

在主页面选择：系统管理>外发配置>邮件配置，进入邮件服务器配置界面，填入邮件服务器地址、端口、邮件地址、密码、邮件主题，提交即可。（告警不支持配置需要授权码进行第三方邮件登录的邮箱，如 QQ、163 邮箱等）

图3-14 邮件服务器配置

表3-5 邮件服务器

参数	说明
邮件服务器地址	此处需填用来发送报警邮件的SMTP服务器地址
邮件地址	用来发送报警邮件的邮件地址
密码	发送报警邮件的邮件地址的密码
发送标题	告警邮件的邮件标题

3.4.2 短信网关配置

告警设置包括邮件告警与短信告警，本系统可以通过设置短信网关通知，在配置完成并保存以后可以通过发送测试短信。确定配置是否正确。

在主页面选择：系统管理>外发配置>短信配置

(1) 选择系统管理>外发配置>短信配置，短信网关配置是短信报警的前提，需要合作的短信平台提供短信告警服务；

(2) 添加短信网关接收短信的网址；

(3) 根据短信网关接收参数的方式，选择提交参数的方法；

(4) 根据短信网关接受的编码方式，选择提交内容的编码方式；

(5) 根据短信平台提供的 API 参数，填写相应的请求参数。

图3-15 短信网关配置

表3-6 默认短信内容参数说明

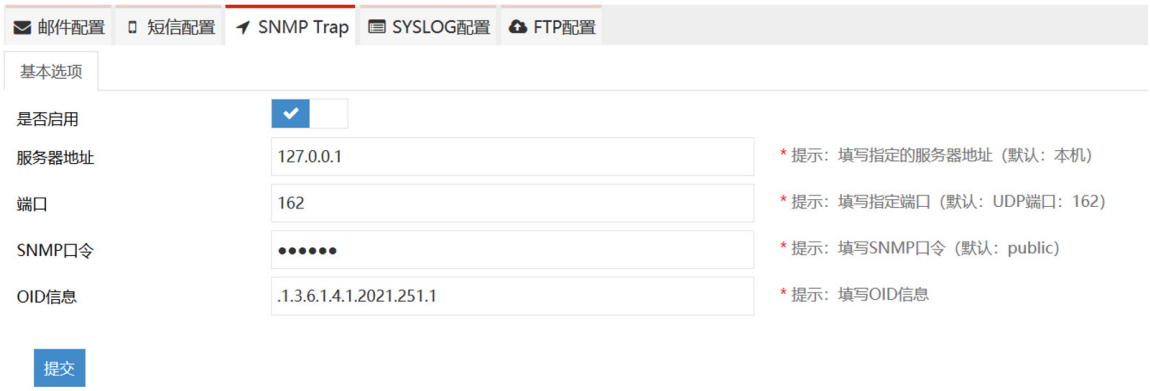
参数	说明
$MESSAGE	为平台内置的告警内容模板，填写请求参数时，无需更改
$MOBILE	为平台内用户的创建告警联系人的手机号码，填写请求参数时，无需更改

3.4.3 SNMPTrap 配置

SNMP 功能是为了方便管理员集中管理设备，对漏洞扫描系统的系统信息，资源及状态等进行统一监控管理。目前支持的协议包括 SNMPv1、SNMPv2，可以同使用标准 SNMP 协议的集中管理软件或设备配合使用。

在配置 SNMP 功能时，用户需要确定使用哪个版本的 SNMP 协议，以便漏洞扫描系统同 SNMP 服务器使用的 SNMP 版本保持一致。

图3-16 SNMPTrap 配置



3.4.4 SYSLOG 配置

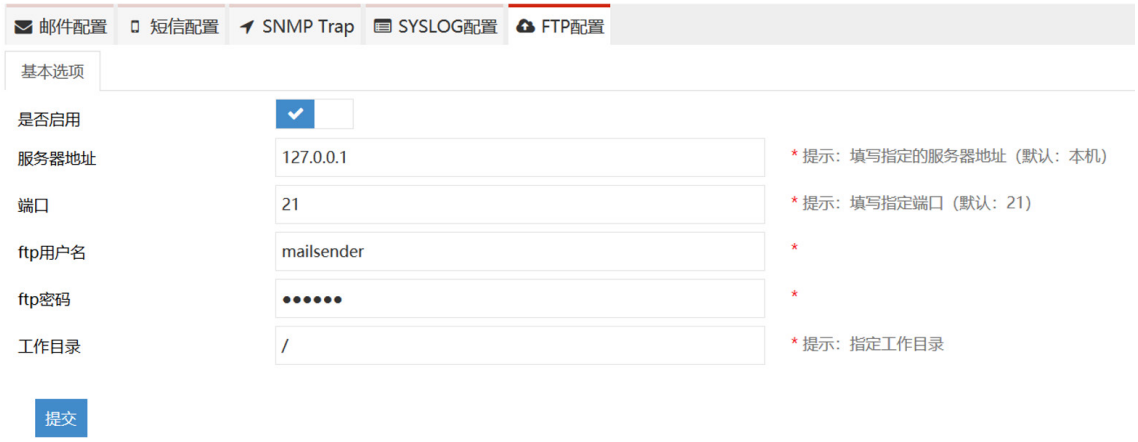
SYSLOG 配置用于指定日志外发的服务器地址，默认使用 UDP 协议的 514 端口。协议、端口配置以自定义，但是必须与日志服务器的配置一致，否则日志服务器将无法接受漏洞扫描系统的日志。

图3-17 SYSLOG 配置

3.4.5 FTP 配置

通过 FTP 配置可将扫描结果保存到 FTP 服务器上，用户需要添加 FTP 服务器地址、端口、FTP 用户名和密码，以及工作目录，并确保漏洞扫描系统到 FTP 服务器可达。

图3-18 FTP 配置



3.5 告警配置

3.5.1 CPU 告警选项

CPU 使用率【百分比】,请输入[1-100]的整数值！写入周期：1 天/次或者模块状态发生变化时写入。

3.5.2 内存告警选项

内存使用率【百分比】,请输入[1-100]的整数值！写入周期：1 天/次或者模块状态发生变化时写入。

3.5.3 磁盘告警选项

磁盘使用率【百分比】,请输入[1-100]的整数值！写入周期：1 天/次或者模块状态发生变化时写入。

3.5.4 网络状态告警选项

开启网络状态告警选项，可以根据网络接口的存在异常则会在下次登录时告警。

3.5.5 设备授权到期告警选项

开启设备授权到期告警选项，若当前时间离授权结束时间不到 30 天（默认 30 天），则会告警。写入周期：1 天/次或者模块状态发生变化时写入。

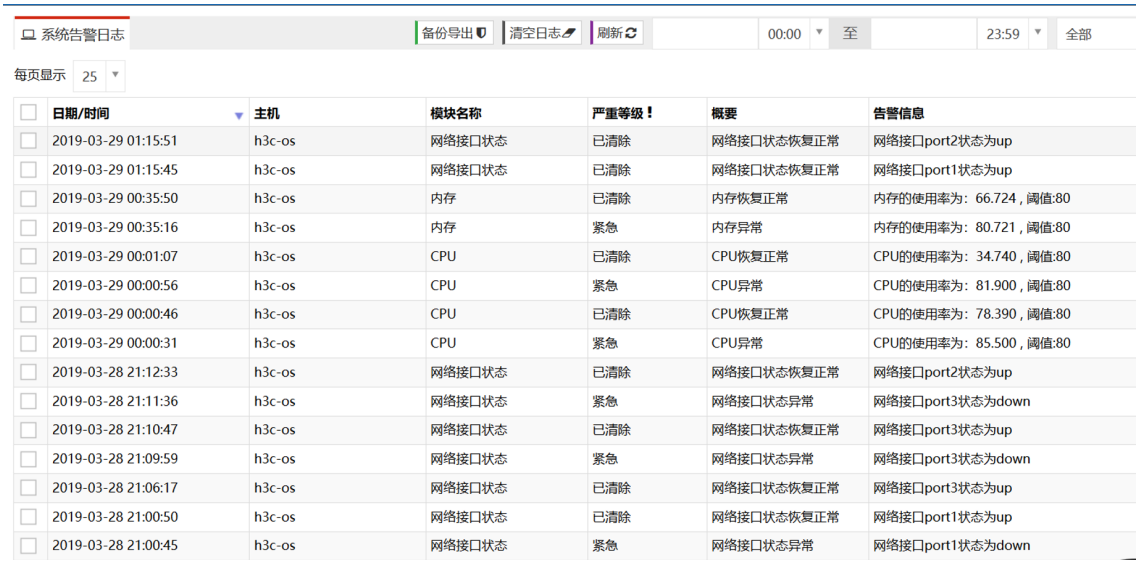
3.5.6 特征库授权到期告警选项

开启特征库授权到期告警选项，若当前时间离授权结束时间不到 60 天（默认 60 天），则会告警。写入周期：1 天/次或者模块状态发生变化时写入。

3.6 系统告警日志

当超出告警配置的值时，会产生告警日志。

图3-19 系统告警日志界面



日期/时间	主机	模块名称	严重等级！	概要	告警信息
2019-03-29 01:15:51	h3c-os	网络接口状态	已清除	网络接口状态恢复正常	网络接口port2状态为up
2019-03-29 01:15:45	h3c-os	网络接口状态	已清除	网络接口状态恢复正常	网络接口port1状态为up
2019-03-29 00:35:50	h3c-os	内存	已清除	内存恢复正常	内存的使用率为：66.724，阈值:80
2019-03-29 00:35:16	h3c-os	内存	紧急	内存异常	内存的使用率为：80.721，阈值:80
2019-03-29 00:01:07	h3c-os	CPU	已清除	CPU恢复正常	CPU的使用率为：34.740，阈值:80
2019-03-29 00:00:56	h3c-os	CPU	紧急	CPU异常	CPU的使用率为：81.900，阈值:80
2019-03-29 00:00:46	h3c-os	CPU	已清除	CPU恢复正常	CPU的使用率为：78.390，阈值:80
2019-03-29 00:00:31	h3c-os	CPU	紧急	CPU异常	CPU的使用率为：85.500，阈值:80
2019-03-28 21:12:33	h3c-os	网络接口状态	已清除	网络接口状态恢复正常	网络接口port2状态为up
2019-03-28 21:11:36	h3c-os	网络接口状态	紧急	网络接口状态异常	网络接口port3状态为down
2019-03-28 21:10:47	h3c-os	网络接口状态	已清除	网络接口状态恢复正常	网络接口port3状态为up
2019-03-28 21:09:59	h3c-os	网络接口状态	紧急	网络接口状态异常	网络接口port3状态为down
2019-03-28 21:06:17	h3c-os	网络接口状态	已清除	网络接口状态恢复正常	网络接口port3状态为up
2019-03-28 21:00:50	h3c-os	网络接口状态	已清除	网络接口状态恢复正常	网络接口port1状态为up
2019-03-28 21:00:45	h3c-os	网络接口状态	紧急	网络接口状态异常	网络接口port1状态为down

3.7 分布式部署

3.7.1 分布式设置

登录 account 账户，在主页面选择：系统管理>分布式部署

(1) 选择系统管理>分布式部署；

(2) 根据实际情况填写相关信息；

(3) 点击提交；

(4) 配置成功后，会在管理中心的引擎列表中查看到子引擎。

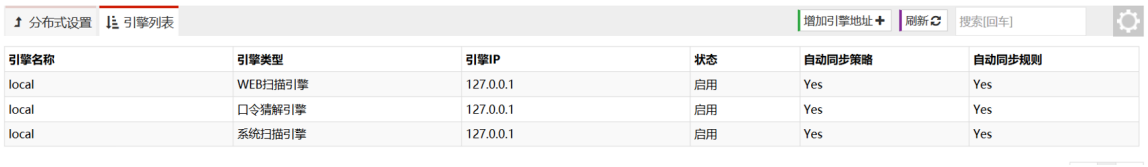
图3-20 分布式部署

表3-7 分布式部署参数说明

参数	说明
管理中心地址	填写需要接入的漏洞扫描系统-管理中心地址
任务分发	管理中心在创建任务时，分配执行该任务的子引擎
引擎名称	在配置分布式引擎时命名的引擎名称，尽量不要跟其它引擎名称冲突

3.7.2 引擎列表

图3-21 引擎列表



3.8 日期时间

NTP 提供漏洞扫描系统与时间服务器进行的同步的功能。通过 NTP 配置，漏洞扫描系统可以从 NTP 服务器上同步漏洞扫描系统的系统时间。

日期/时间类型：手工配置适用于内网环境。若设备在公网环境下将会自动同步标准时间。

通用的服务器地址：填写正确的时间服务器地址。

图3-22 日期/时间

3.9 配置备份恢复

备份主要是针对漏洞扫描系统配置文件的备份。建议用户定期对漏洞扫描系统的配置信息进行备份，以供将来恢复系统配置时使用。另外备份数据还可以导入导出系统，这样增加了系统的可靠性。

图3-23 配置备份恢复

3.10 漏洞检测备份

备份当前系统漏洞检测信息。

图3-24 漏洞检测备份

可对备份的文件进行删除和下载操作。

图3-25 漏洞检测备份操作

3.11 版本/特征库升级

升级是对漏洞扫描系统版本的管理，分为整个系统的升级、特征库升级。

3.11.1 自动升级

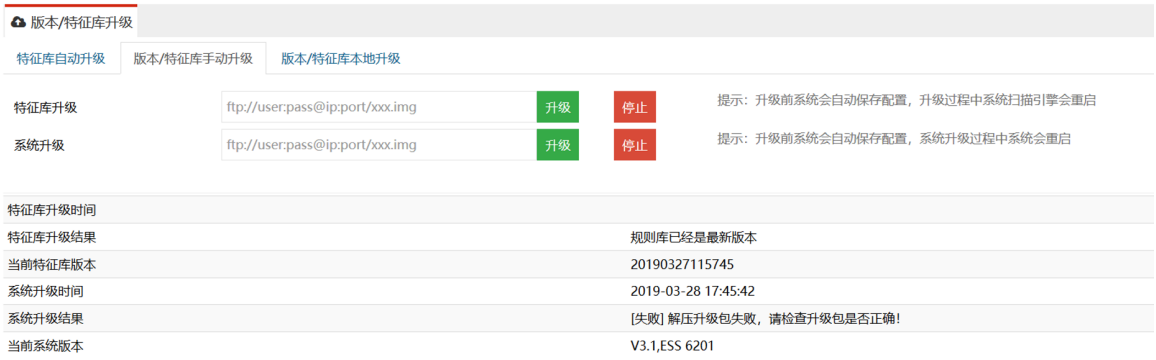
主要针对系统的特征库进行升级，需要填写升级服务器地址，访问服务器地址的用户名和密码，并选择执行周期可以设置每天执行，每周执行，每月执行进行自动升级。

图3-26 自动升级

3.11.2 手动升级

如果要对特征库和系统升级，需要下载特征库包或者系统升级包，搭建 FTP 服务器根据命令 ftp://user:pass@ip:port/xxx.img 进行升级。

图3-27 手动升级



3.11.3 本地升级

在本地下载好特征库升级包或系统升级包后，直接点击导入选择包等待上传，在上传过程中可以看到上传进度。

图3-28 本地升级

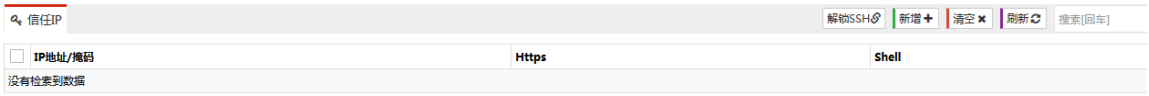
3.12 信任IP

使用该功能可以设置 IP 网段对漏洞扫描系统进行管理。同时也可以设定允许访问的类型，如 Https、Shell。

HTTPS：是否允许上面设置的网段的机器访问漏洞扫描系统的 HTTPSWeb 服务。

Shell：是否允许上面设置的网段的机器访问漏洞扫描系统的 WebShell 服务。

图3-29 信任 IP 配置



3.13 诊断工具

诊断工具包含 PING 命令、WEBGET 命令、端口探测工具、Tcpdump 抓包工具以及故障信息收集。一键诊断功能能快速对 PING、DNS、WEBGET 进行检测。

在主页面选择：系统管理>诊断工具，进入诊断工具，进行相应的配置。

- PING 命令

  测试系统与远程主机之间的连通性。

- WEBGET 命令

  测试网站能否被平台正常访问。

- 端口探测工具

  测试远程主机端口是否开放。

- Tcpdump 抓包工具

  抓包检测流量传输情况。

- 故障信息收集

  对发生故障的信息进行收集。

图3-30 PING 命令

图3-31 WEBGET 命令

图3-32 端口探测工具

图3-33 Tcpdump 抓包工具

图3-34 故障信息收集

3.14 验证工具

3.14.1 通用验证

验证工具主要提供两个验证工具，一个是通用验证，一个是 SQL 注入验证，SQL 注入验证是专门针对注入类漏洞的验证工具，通用验证是针对除注入类漏洞外的其它 web 漏洞的验证工具。通过这两类验证工具可以直接手动添加 URL 和问题参数进行验证，主要是用来针对平台 web 扫描扫描出的漏洞进行验证可以直接将漏洞 URL 和参数同步到验证工具中的 URL 和参数中进行验证。

图3-35 通用验证

3.14.2 SQL 注入验证

在主页面选择：系统管理>验证工具>SQL 注入验证

能够进行一些 SQL 注入验证操作，正确填写参数后点击<验证>，即可验证

图3-36 SQL 注入验证

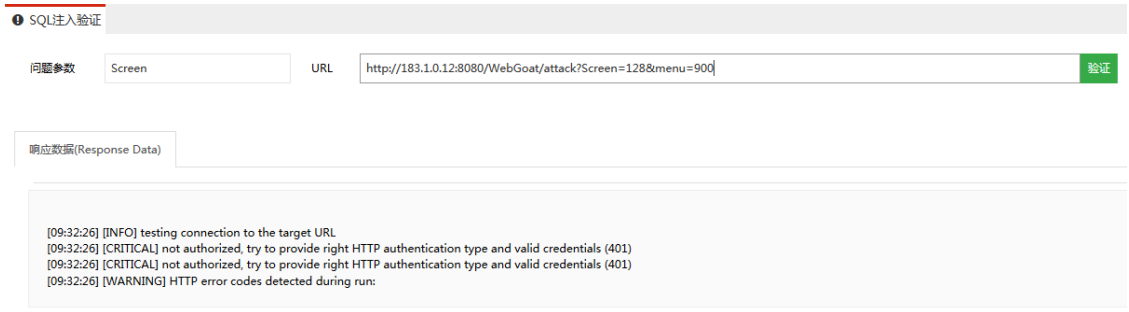
一般来说，扫描出网站漏洞后在网站详情查询中，可以查看漏洞详情

漏洞详情页面中点击 SQL 注入验证

图3-37 漏洞详情

此时会跳转到通用验证页面，显示如下

图3-38 SQL 注入验证页面



3.15 SNMP管理

图3-39 snmp 管理 snmpv3 协议界面

表3-8 用户管理参数说明

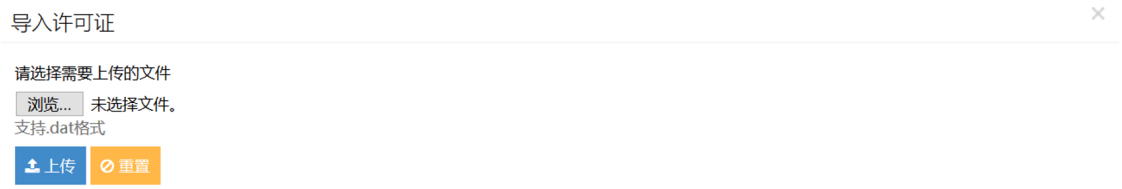
参数	说明
SNMP版本	可选择snmpv3或snmpv1c/snmpv2c。使用snmpv1c/snmpv2c不安全
SNMPV3用户名	填写SNMPV3用户名
SNMPV3密码	密码要求：【字母、数字、特殊符号、长度在[8-32]之间的组合密码】。示例：access12@1
密码哈希算法	选择加密码算法
加密口令	输入加密口令
允许访问IP/网段	允许访问的ip或网段，以，隔开，网段示例：192.168.1.0/24
协议公共体	SNMPv1SNMPv2c协议公共体，当不配置该项或为空时，禁用SNMPv1SNMPv2c

4 许可证管理

登录 account 账户，在主页面选择：license 管理，进入 license 管理页面

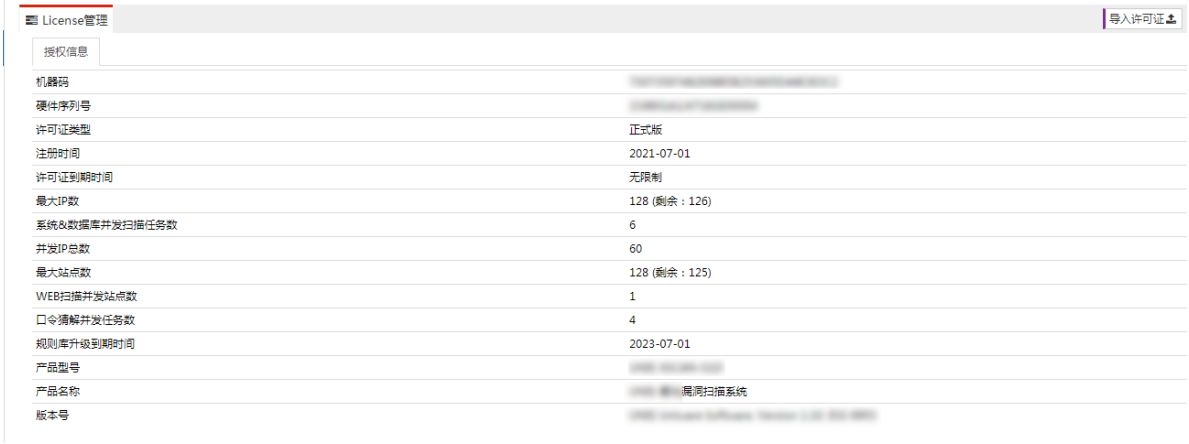
点击导入许可证可将获得的许可证文件导入；

图4-1 导入许可证



授权导入成功后，重新登录可查看授权信息。

图4-2 查看授权信息



5 策略模板

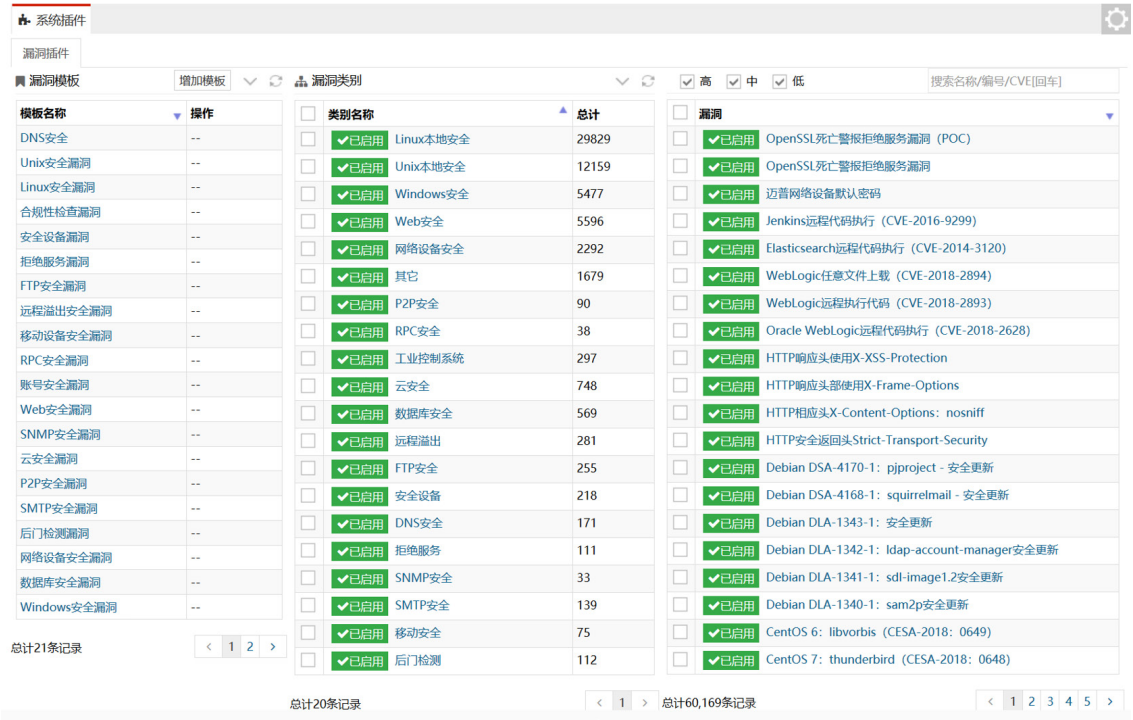
策略模板是基于脚本的规则库，包括系统插件和 web 插件，其中系统漏洞检测插件 20 多类，60000 多条；web 漏洞检测插件共覆盖 OWASP 定义的 10 大类漏洞规则，且覆盖了 CVE、CNVD、CNNVD、CNCVE、Bugtraq 等多个漏洞库中的所有漏洞。我们将定期发布最新的规则库，用户可以通过公司官方网站获得最新的规则库。

5.1 系统插件

系统漏洞插件库

系统内置全面的漏扫扫描插件，可以灵活的定义扫描策略。

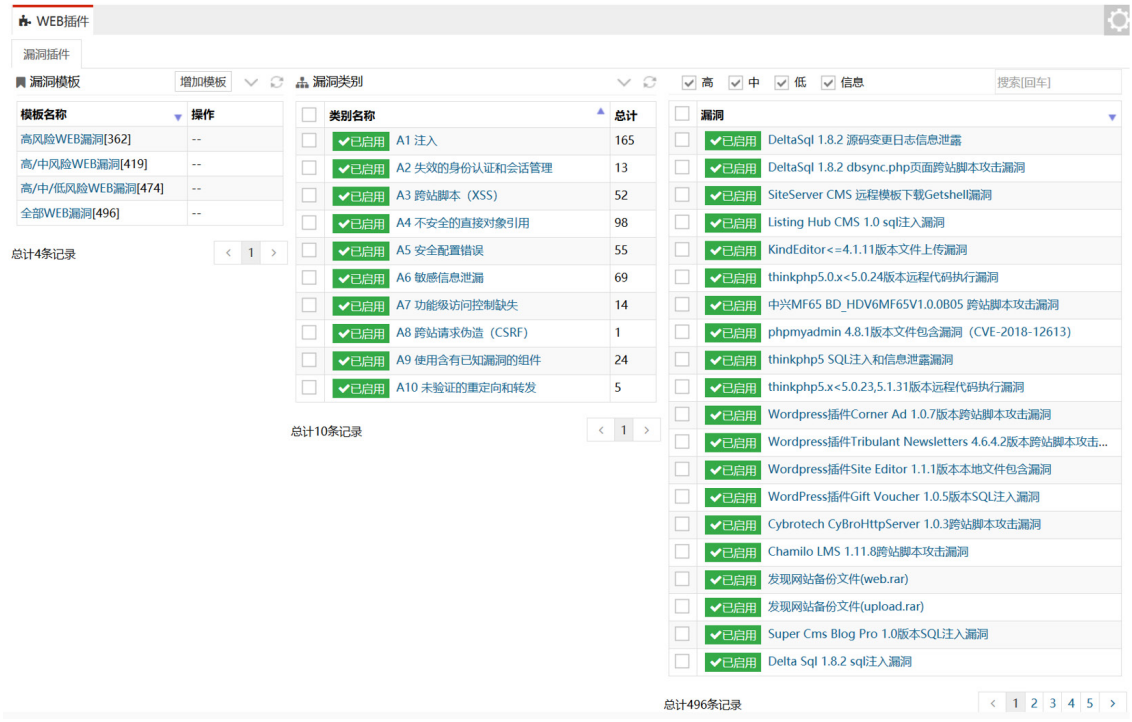
图5-1 系统漏洞插件库



5.2 WEB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。

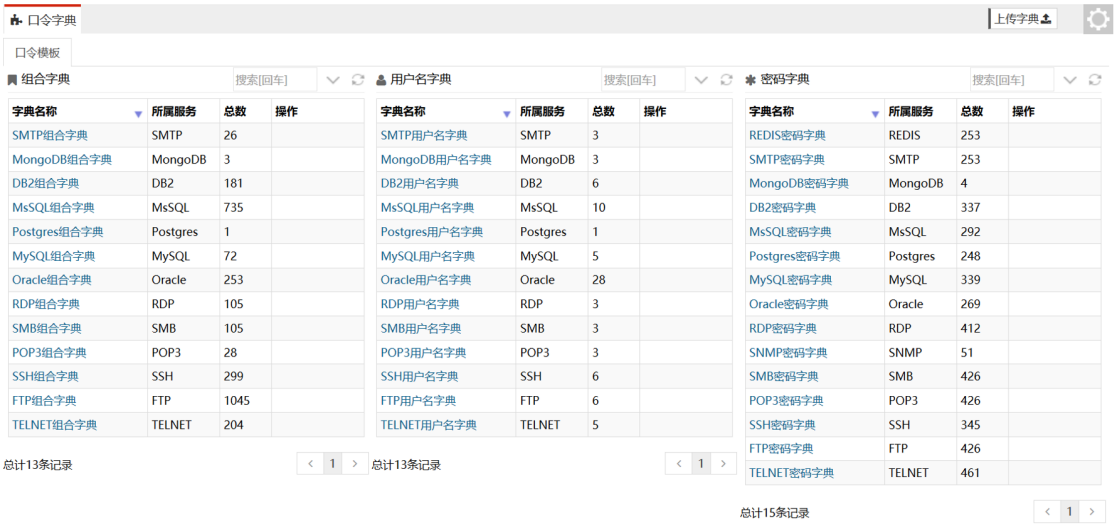
图5-2 web 漏洞插件库



5.3 口令字典

有系统默认的口令字典组合模式模板和单独的用户名字典模板和密码字典，也可以自定义字典按照文件内容特征和所属服务类型进行上传字典。

图5-3 口令字典



6 任务中心

6.1 新建任务

6.1.1 系统漏洞扫描任务

1. 扫描基本配置

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 添加漏洞扫描任务

扫描目标：

输入的内容有[单个主机]和[主机组]两种，多个之间以英文逗号(,)或换行分隔。

单个主机示例：192.168.1.100，也可使用域名：www.example.com，

IPv6 示例：2001:fecd:ba23:cd1f:dcb1:1010:9234:4088，

主机组示例：192.168.1.0/24,192.168.2.1-254,192.168.3.1-192.168.3.254；

排除某个 IP：192.168.1.0/24!192.168.1.100。

任务名称：

填写新建的系统扫描任务名称。

执行方式：

选择立即执行/定时执行一次/每天执行一次/每周执行一次/每月执行一次。

检测模式：

完全扫描：采用主机存活判断、端口扫描、服务判断、漏洞测试的步骤对扫描目标进行完整的安全扫描。强制扫描：使用强制手段对扫描目标进行主机存活、端口服务探测。登录审计：利用配置好的用户名密码列表对主机进行登录后的本地审计

漏洞插件模板：

选择漏洞插件模板

分布式引擎：

可选择默认/local，两台及以上数量的设备协同工作的一种部署方式，其中一台作为管理中心，其它的设备作为引擎，管理中心统一进行任务调度及结果展示等操作，管理中心可同时做任务调度和作为分布式引擎使用。默认：系统将根据引擎的负载情况，智能选择工作引擎。同时也可以指定引擎。

执行优先级：

当任务达到并发上限时，‘排队等待’级别高的任务将优先执行。可选择高/中/低。

检测结束发送邮件：

需要在告警配置中配置邮件网关，多个邮箱可用英文逗号（,）分割。

检测结束发送短信：

需要在告警配置中配置了短信网关，多个手机号码可用英文逗号（,）分割。

2. 自主选择插件

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6-2 漏洞扫描-自主选择插件

3. 探测选项

图6-3 漏洞扫描-探测选项

提示扫描目标

在扫描之前提示被扫主机，需要扫描目标支持 messager 服务。

开启存活探测

如果开启，引擎使用如下探测方法进行探测，如果不能确定存活，则不进行探测，提高检测速度；如果不开启，则对所有主机进行漏洞检测，会延长检测时间。

主机存活测试

可以复选 ARP、ICMP PING、TCP PING、UDP PING。默认选择前三种。

端口扫描范围

可以选择：标准、快速、全部、指定。

标准：默认端口 4000 多个。快速：100 个常用端口。全部：端口 0-65535。

指定：单个或范围如 22，1-1024，指定 TCP 端口：TCP:1024-65535，制定 UDP 端口：UDP:1025-65535。

端口扫描方式

CONNECT 方式为全连接扫描，完成 TCP/IP 的三次握手，速度较慢。SYN 方式，只需要发送 TCPSYN 包即可完成检测，速度快，建议使用 SYN。

4. 检测选项

图6-4 漏洞扫描-检测选项

最大限度报告漏洞

若选择关闭，则将大大提高扫描速率，部分耗时长的规则将跳过执行。

执行所有规则检测

若选择开启：检测耗时越久、对检测目标的覆盖面更广。

执行相关联漏洞

若选择开启：某些已例外的漏洞将加入到扫描结果当中。

保存漏洞检测详情

若选择开启：漏洞的详细打印信息将加入到扫描结果当中。

自适应网络

根据网络的反应速度，适当调整发包的速率，从而不至于将网络扫瘫痪，但会影响扫描速度

危险测试

包含一些危险的测试方法，如：拒绝服务检测，导致扫描目标的拒绝服务，因此慎用。

停止探测无响应的主机

如果扫描过程中发现扫描目标没有反应，停止对该目标的探测。

启用口令破解

使用默认字典对系统或服务的口令进行猜解。

测试 Oracle 账号

对 Oracle 数据库进行深度检测。

启用 Web 检测

开启则可进行 web 检测。

SMB 信息探测

启用则可进行 SMB 信息检测。

5. 引擎选项

图6-5 漏洞扫描-引擎选项

插件超时

单个插件执行时间最长设置[10-300]。

网络时延

网络连接超时设置[10-300]。

单个主机检测并发数

针对单个的检测目标，并发的检测插件数量[1-50]。

单个扫描任务并发主机数

单个扫描任务，可同时扫描的主机数量[1-120]。注：根据型号不同，最大并发主机数有差异。

单个主机 TCP 连接数：

针对单个检测目标，并发的 TCP 连接数量[1-1024]。

单个扫描任务 TCP 连接数：

单个扫描任务，最多可同时并发的 TCP 连接数[1-1024]。

6. 登录信息选项

图6-6 漏洞扫描-登录信息选项

预设登录账号

下拉选择 SSH、SMB、TELNET、POP、POP3、IMAP、FTP、RSH、REXEC、WSUS、SNMP、RDP 共 12 种，主要选择主机相应的服务并填写用户名密码，再进行登录验证，提交扫描即可；

数据库类型

下拉选择 None、Postgres、Oracle、Mysql、Mssql、DB2、Informix、Sybase。选择需要检测的主机上的数据库类型，填写相对应的端口，用户名，密码提交即可，目前数据库验证支持 PostgreSQL、MsSQL、MySQL 认证；

登录验证

下拉选择 TELNET、SSH、SMB、RDP 共 4 种，登录扫描验证。

图6-7 登录验证

数据库验证

下拉选择 Postgres、MySqpl、MsSql 共 3 种，数据库登录扫描验证。

图6-8 数据库验证

微软 WSUS 账号

WSUS 是个微软推出的网络化的补丁分发方案。通过对 WSUS 账号配置与 WSUS 服务器建立连接，从 WSUS 获取补丁信息，或者反馈给 WSUS 哪些 Windows 主机缺少哪些补丁，在报表中显示获取的补丁信息。

图6-9 WSUS 账号

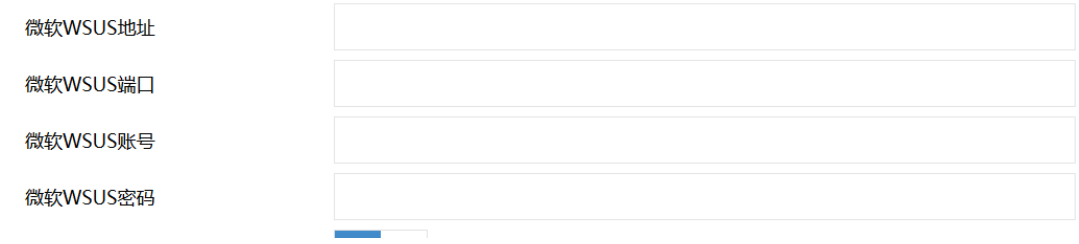


表6-1 WSUS 账号参数说明

参数	说明
微软WSUS地址	填写微软WSUS地址
微软WSUS端口	填写微软WSUS端口
微软WSUS账号	填写微软WSUS账号
微软WSUS密码	填写微软WSUS密码

https 参数

与 WSUS 通信使用 http 协议或 https 协议，勾选代表使用 https 协议，否则代表使用 http 协议。

图6-10 https 参数

6.1.2 Web 漏洞扫描任务

1. 扫描基本配置

针对 web 扫描，添加需要扫描的目标，填写形式为单个站点或者站点组，配置任务名称，选择 web 扫描插件模板并提交扫描。

图6-11 添加任务

扫描目标

URL 地址：http://www.example.com/或 https://www.example.com/*URL 地址：http://192.168.1.100/或 https://192.168.1.100/*IPv6URL 示例：http://[2001:fecd:ba23:cd1f:dcb1:1010:9234:4088]/*多个 URL 以英文逗号(,)或回车分隔。

任务名称

填写新建的 WEB 扫描任务名称。

执行方式

选择立即执行/定时执行一次/每天执行一次/每周执行一次/每月执行一次。

漏洞插件模板

选择漏洞插件模版。

分布式引擎

可选择默认/local。两台及以上数量的设备协同工作的一种部署方式，其中一台作为管理中心，其它的作为引擎，管理中心统一进行任务调度及结果展示等操作，管理中心可同时做任务调度和作为分布式引擎使用。默认：系统将根据引擎的负载情况，智能选择工作引擎。同时也可以指定引擎。

执行优先级

当任务达到并发上限时，排队等待中'级别高的任务将优先执行。可选择高/中/低。

检测结束发送邮件

需要在告警配置中配置了邮件网关，多个邮箱可用英文逗号(,)分隔。

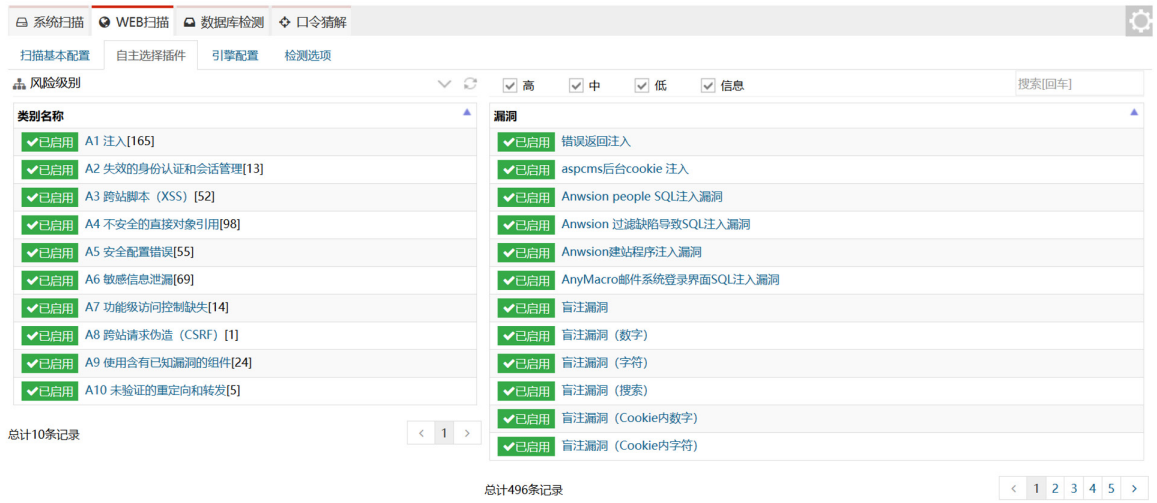
检测结束发送短信

需要在告警配置中配置了短信网关，多个手机号码可用英文逗号(,)分隔。

2. 自主选择插件

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6-12 WEB 扫描-自主选择插件



3. 引擎配置

图6-13 WEB 扫描-引擎配置

并发线程数

单个扫描目标，并发执行的线程数量[1-20]。

区分大小写

网站对于 Url 中字母大小写是否敏感。

最大类似页面数

引擎用于归并类似链接时需要保留类似链接的数量[1-1000]。

同目录下最大页面数

引擎在归并链接时，同一目录下需要保留的链接数量[1-1024]。

重试次数

当链接无法访问时，重新访问的次数[1-10]。

超时时间

当访问链接时超过多长时间，判定链接无法访问[1-300]。

代理类型

网站访问目标网站时，可能需要通过代理才能访问，代理类型有 2 种：HTTP、SOCKS。

图6-14 HTTP 代理

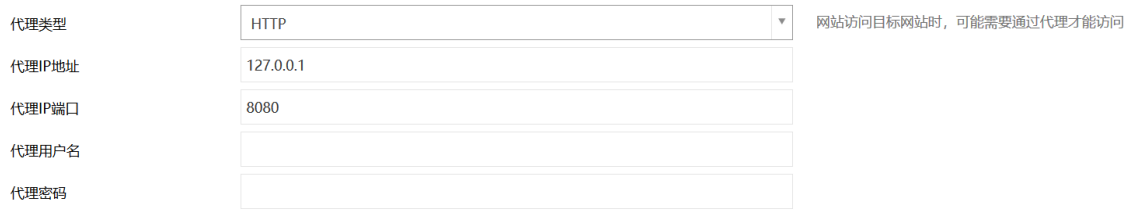
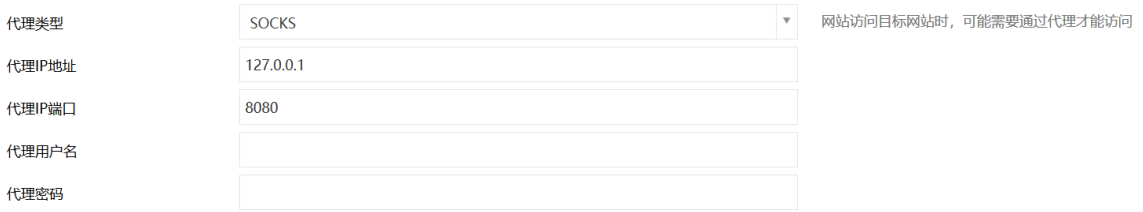
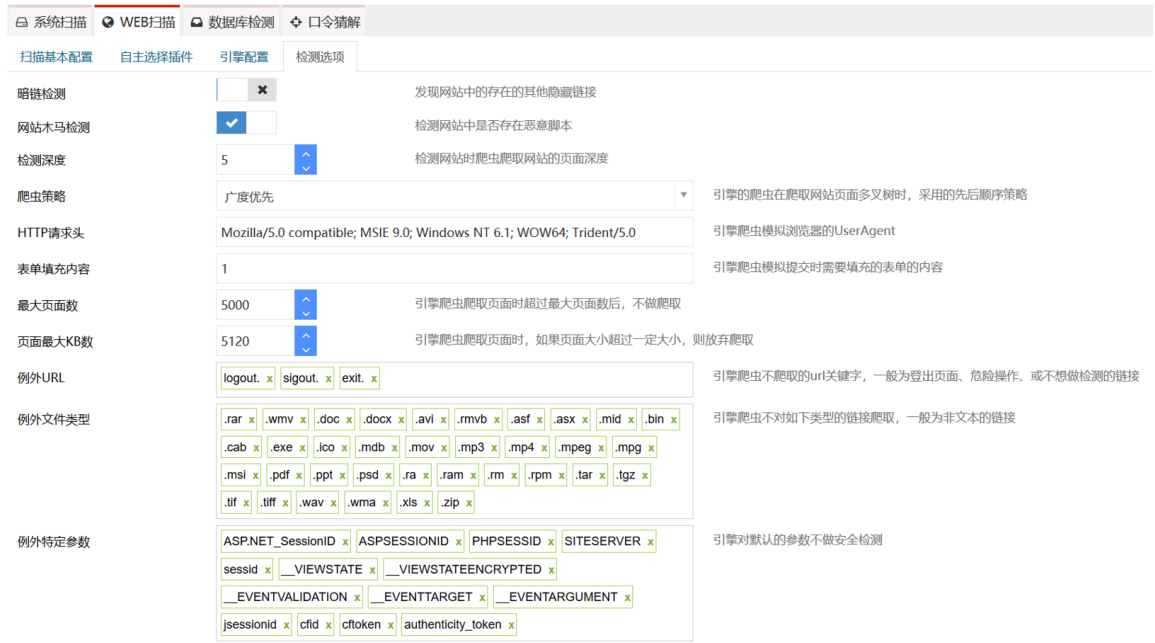


图6-15 SOCKS 代理



4. 检测选项

图6-16 WEB 扫描-检测选项



暗链检测

发现网站中的存在的其它隐藏链接.

网站木马检测

检测网站中是否存在恶意脚本。

检测深度

检测网站时爬虫爬取网站的页面深度。

爬虫策略

引擎的爬虫在爬去网站页面多叉树时，采用的先后顺序策略：广度优先和深度优先。广度优先指横向爬取，又叫层次遍历，从上往下对每一层依次访问，在每一层中，从左往右（也可以从右往左）访问结点，访问完一层就进入下一层，直到没有结点可以访问为止。深度优先指纵向爬取，是对每一个可能的分支路径深入到不能再深入为止，而且每个结点只能访问一次。

Http 请求头

引擎爬虫模拟浏览器的 UserAgent。

表单填充内容

引擎爬虫模拟提交时需要填充的表单的内容。

最大页面数

引擎爬虫爬去页面时超过最大页面数后，不做爬取。

页面最大 KB 数

引擎爬虫爬去页面时，如果页面大小超过一定大小，则放弃爬去。

例外 URL

引擎爬虫不爬取的 url 关键字，一般为登出页面、危险操作、或不想坐检测的链接。

例外文件类型

引擎爬虫不对如下类型的链接爬取，一般为非文本的链接。

例外特定参数

引擎对默认的参数不做安全检测。

6.1.3 数据库扫描任务

1. 扫描基本配置

针对数据库扫描，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，选择数据库扫描插件模板并提交扫描。

图6-17 添加数据库扫描任务

扫描目标

*输入的内容有单个主机和主机组两种，多个之间以英文逗号,或换行分隔。

*单个主机示例：192.168.1.100 也可使用域名：www.example.com。

*IPv6 示例：2001:fecd:ba23:cd1f:dcb1:1010:9234:4088。

*主机组示例：192.168.1.0/24,192.168.2.1-254,192.168.3.1-192.168.3.254。

*排除某个 IP：192.168.1.0/24!192.168.1.100。

数据库类型

可下拉选择：None、Postgres、Oracle、MySQL、msSQL、DB2、Informix、Sybase。

任务名称

填写新建的数据库扫描任务名称。

执行方式

选择立即执行/定时执行一次/每天执行一次/每周执行一次/每月执行一次。

漏洞插件模板

选择数据库漏洞插件模板。

分布式引擎

可选择默认/local。两台及以上数量的设备协同工作的一种部署方式，其中一台作为管理中心，其它的作为引擎，管理中心统一进行任务调度及结果展示等操作，管理中心可同时做任务调度和作为分布式引擎使用。默认：系统将根据引擎的负载情况，智能选择工作引擎。同时也可以指定引擎。

执行优先级

当任务达到并发上限时，'排队等待中'级别高的任务将优先执行。可选择高/中/低。

检测结束发送邮件

需要在告警配置中配置了邮件网关，多个邮箱可用英文逗号(,)分隔。

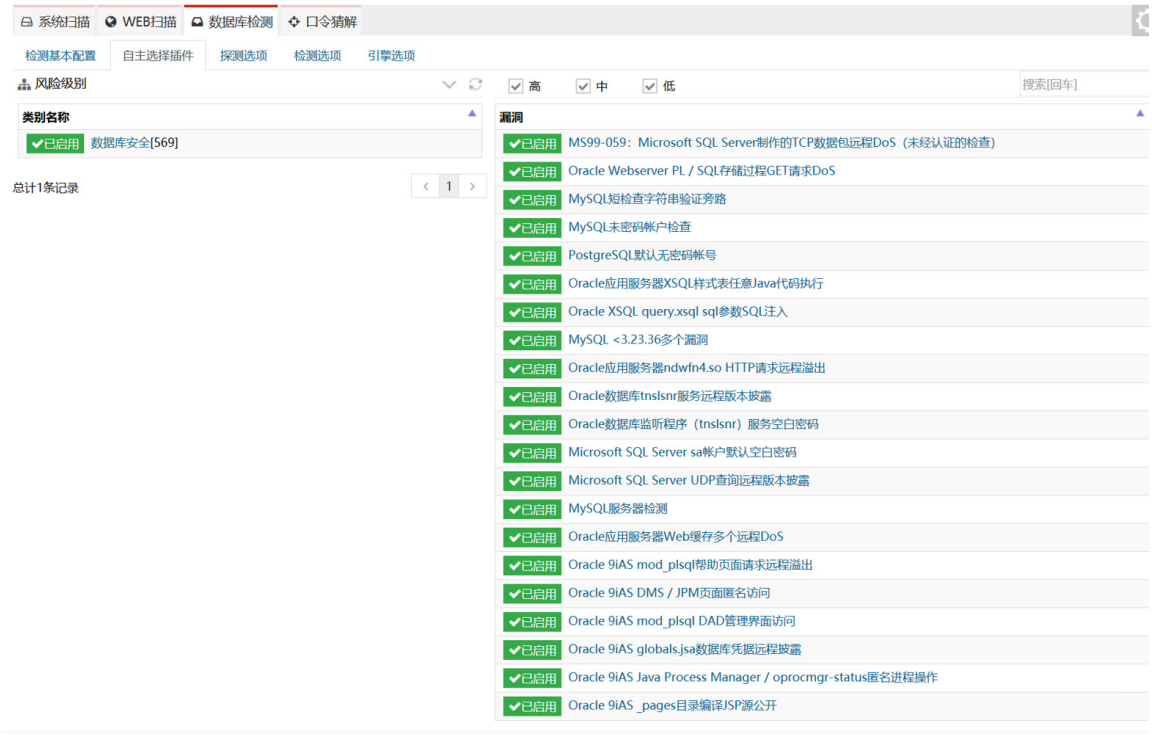
检测结束发送短信

需要在告警配置中配置了短信网关，多个手机号码可用英文逗号(,)分隔。

2. 自主选择插件

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6-18 数据库扫描-自主选择插件



3. 探测选项

图6-19 数据库扫描-探测选项

提示扫描目标

在扫描之前提示被扫描主机，需要扫描目标支持 messager 服务。

开启存活探测

如果开启，引擎使用如下探测方法进行探测，如果不能确定存活，则不进行检测，提高检测速度；如果不开启，则对所有主机进行漏洞监测，会延长检测时间。

主机存活测试

可以复选 ARP、ICMPPING、TCPPING、UDPPING。默认选择前三种。

端口扫描范围

标准：默认端口 4000 多个。快速：100 个常用端口。全部：端口 0-65535，指定：单个或范围如 22,1-1024，指定 TCP 端口：TCP:1024-65535,指定 UDP 端口：UDP:1025-65535。

端口扫描方式

CONNECT 方式为全连接扫描，完成 TCP/IP 的三次握手，速度较慢。SYN 方式，只需要发送 TCPSYN 包即可完成检测，速度快，建议使用 SYN。

4. 检测选项

图6-20 数据库扫描-检测选项

最大限度报告漏洞

若选择关闭，则将大大提高扫描速率，部分耗时长的规则将跳过执行。

执行所有规则检测

若选择开启：检测耗时越久、对检测目标的覆盖面更广。

执行相关联漏洞

若选择开启：某些已例外的漏洞将加入到扫描结果当中。

保存漏洞检测详情

若选择开启：漏洞的详细打印信息将加入到扫描结果当中。

自适应网络

根据网络的反应速度，适当调整发包的速率，从而不至于将网络扫瘫痪，但会影响扫描速度。

危险测试

包含一些危险的测试方法，如：拒绝服务检测，导致扫描目标的拒绝服务，因此慎用。

停止探测无响应的主机

如果扫描过程中发现扫描目标没有反应，停止对该目标的探测。

启用口令破解

使用默认字典对系统或服务的口令进行猜解。

测试 Oracle 账号

对 Oracle 数据库进行深度检测。

启用 Web 检测

开启则可进行 Web 检测。

SMB 信息探测

启用则可进行 SMB 信息检测。

5. 引擎选项

图6-21 数据库扫描-引擎选项

插件超时

单个插件执行时间最长设置[10-300]。

网络时延

网络连接超时设置[10-300]。

单个主机检测并发数

针对单个的检测目标，并发的检测插件数量[1-50]。

单个扫描任务并发主机数

单个扫描任务并发主机数。注：根据漏扫不同型号最大并发主机数会有差异。

单个主机 TCP 连接数

针对单个检测目标，并发的 TCP 连接数量[1-1024]。

单个扫描任务 TCP 连接数

单个扫描任务，最多可同时并发的 TCP 连接数[1-1024]。

6.1.4 口令猜解任务

1. 扫描的基本配置

针对口令猜解任务是基于资产的，首先需要选择资产，自定义任务名称，选择执行方式，选择扫描的服务类型和数据库类型，其中检测模式有两种，标准模式和组合模式，标准模式是指只针对用户

名或密码一项扫描，组合模式是针对用户名和密码一起进行扫描。针对字典可以选择系统自带的默认字典也可以自定义按照相应格式上传自定义字典进行扫描，再填写相对应的端口号提交即可。

图6-22 口令猜解任务基本配置

2. 引擎选项

图6-23 口令猜解任务—引擎选项

口令猜解速率

对单个服务进行口令猜解的探测速度，值越小，探测速度越慢。值越小，目标主机对引擎的阻断概率越小。

最大线程并发数

对单个服务进行口令猜解的并发线程数，值越大，探测速度越快。

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6-24 任务列表-任务列表

任务列表中，各项参数含义如下：

任务名称

显示当前任务的名称，格式为用户在添加任务时的命名。

执行方式

执行方式分为手动执行、定时执行、每日执行、每周执行、每月执行、离线执行。

开始时间/结束时间

显示当前评估任务的开始和结束时间，对于尚未结束的任务，只显示其开始时间。

操作

可以选择立即开始或者禁用当前任务，对于正在执行的任务，可以选择暂停或者停止该任务。

检测耗时

可以实时的展示出任务执行检测大致需要的执行时间，执行完成会显示整个任务扫描花费的时长。

进度

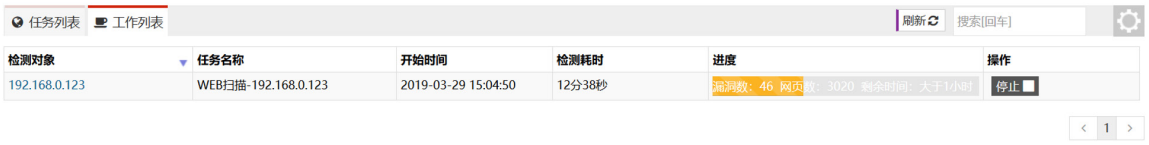
显示当前任务执行的进度情况，点击进度栏可以查看当前任务的漏洞数，资产组的主机漏洞排名，风险等级分布及历史执行记录。

图6-25 任务列表-任务列表进度

6.3 工作列表

工作列表主要展示了当前开启的任务中正在执行的任务。可以看到该任务的任务名称，开始时间，检测耗时以及执行的进度。也可以对正在执行的任务进行暂停或停止操作。

图6-26 任务列表-工作列表



工作列表中，各项参数含义如下：

检测对象

显示当前任务中里包含的检测对象。

任务名称

显示当前任务的名称，格式为用户在添加任务时的命名。

开始时间

显示当前评估任务的开始时间。

检测耗时

可以实时的展示出任务执行检测大致需要的执行时间，执行完成会显示整个任务扫描花费的时长。

进度

显示当前任务执行的进度情况，如果是 web 扫描可以展示漏洞数，网页数，剩余时间，如果是系统扫描会展示漏洞数，主机数，剩余时间。

操作

对于正在执行的任务，可选择停止/强制停止当前任务。

6.4 探测未知站点

探测未知站点是扫描 IP 范围内可能存在的 web 站点。

6.4.1 新建探测任务

图6-27 探测未知站点-新建探测任务

探测端口范围

填写 web 站点常用的端口及自定义端口。

6.4.2 探测详情

图6-28 探测未知站点-探测详情

转成任务

自动跳转到 web 漏洞扫描，将探测出的 web 站点添加到扫描目标中。

转成资产

自动添加资产，提交到资产组中。

6.5 会话录制

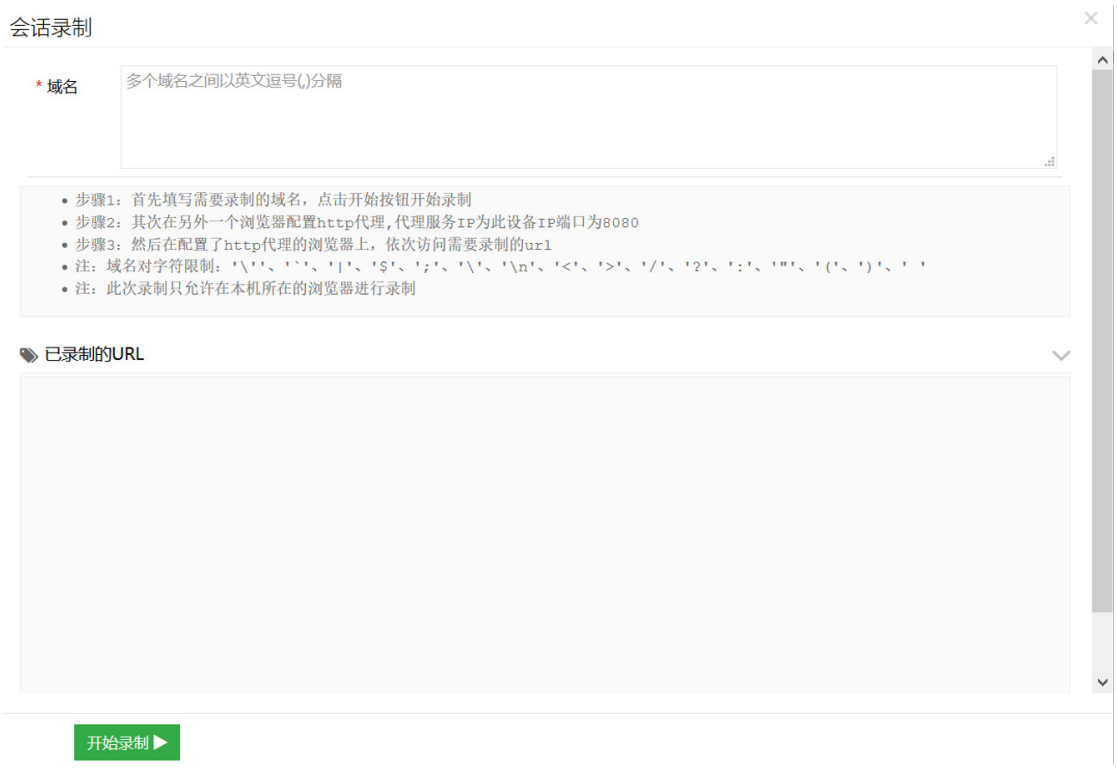
6.5.1 开始录制会话

首先填写需要录制的域名，点击开始按钮开始录制，其次在另外一个浏览器配置 http 代理,代理服务 IP 为此设备 IP 端口为 8080，然后在配置了 http 代理的浏览器上，依次访问需要录制的 url。

注：域名对字符限制：'\"、'`'、'|'、'$'、';'、'\'、'\n'、'<'、'>'、'/'、'?'、':'、'"'、'('、')'、"

注：此次录制只允许在本机所在的浏览器进行录制

图6-29 录制会话界面



6.5.2 停止会话

将正在录制的会话停止。

6.5.3 保存会话

将已录制的会话保存。

6.5.4 录制的会话列表

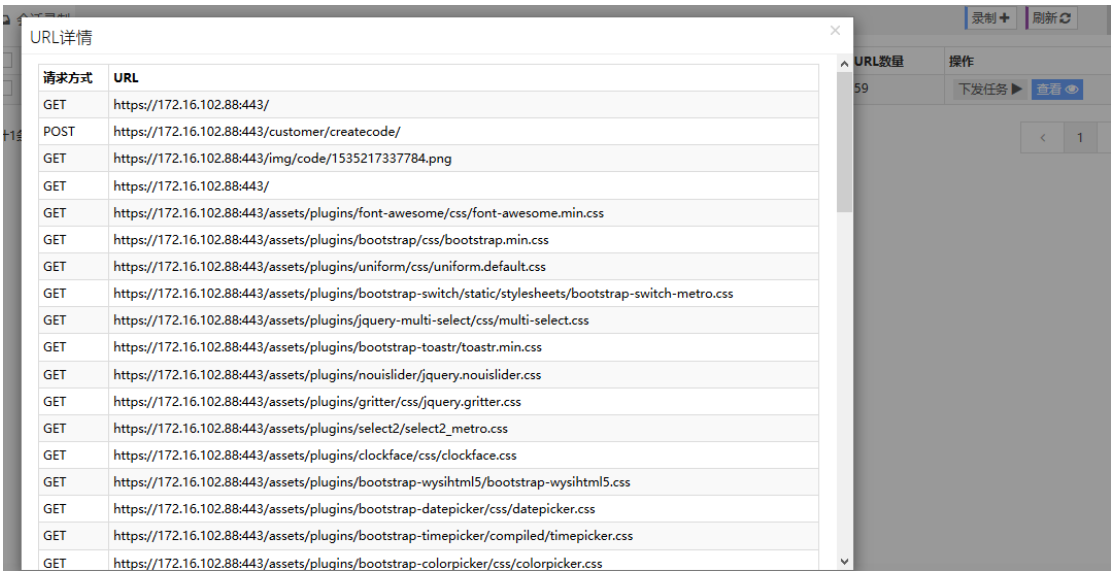
图6-30 会话录制列表

6.5.5 下发任务

将已录制的会话下发 web 扫描任务。

6.5.6 查看录制的会话内容

图6-31 查看录制



7 资产管理

管理员可以对所有资产设备进行风险资产管理，在进行资产风险管理时，首先需要创建资产。通过资产，管理员可以浏览网内全部资产的数量以及资产的安全情况。

图7-1 资产管理

对于其中一个资产，点击可以显示资产树，管理员可以通过查看资产树来了解自己的网络资产情况。

系统扫描资产：点击系统扫描资产中的资产会显示该资产的资产风险，漏洞详情及资产指纹信息以及系统资产组属性。资产风险描述了每个资产不同执行时间段的漏洞数，具体到高、中、低危的风险；漏洞详情描述了每个漏洞的具体信息；资产信息描述了每个资产的主机信息；系统资产属性主要描述了该资产所属的资产名称，及其扫描 IP/域名。

图7-2 系统资产管理-资产详情

Web 扫描资产：点击 web 扫描资产中的一条资产会在页面右边显示出该资产的资产风险，漏洞详情，资产信息，资产属性；资产风险描述了每个资产不同执行时间段的漏洞数，具体到高、中、低危的风险；漏洞详情描述了每个漏洞的具体信息；资产信息描述了每个 web 资产的详细信息；资产属性主要描述了该资产所属的资产名称，起始 URL，其它 URL，网站域名，扫描根目录，例外 URL，登录认证。其中资产名称，起始 URL，网站域名会扫描完该资产后自动同步，至于其它 URL，网站域名，例外 URL，登录认证（Cookie 认证，Form 认证，Basic 认证，NTLM 认证）需要用户根据资产需要进行自主配置。

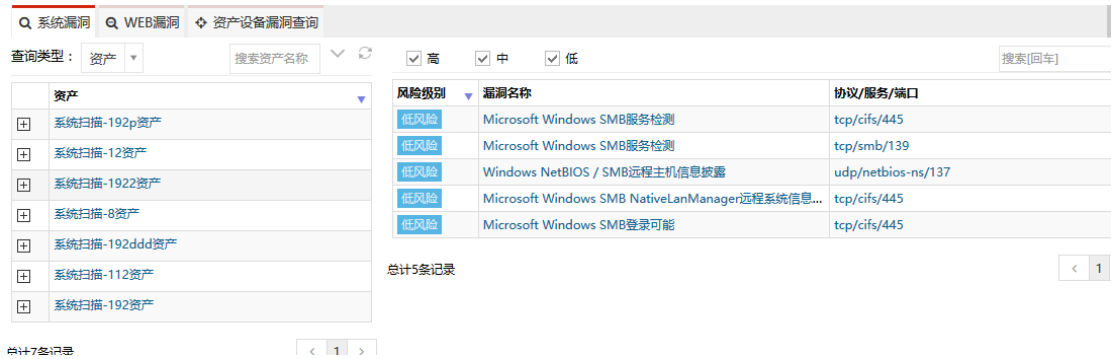
图7-3 web 资产管理-资产详情

8 报表管理

8.1 在线查询

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。还可以选择查询系统漏洞/WEB 漏洞/资产设备漏洞。

图8-1 在线查询



8.2 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。还可以进行资产组之间的漏洞对比。

图8-2 对比分析

8.3 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、PDF,EXCEL、XML，报表标题可自定义。

图8-3 导出扫描报表

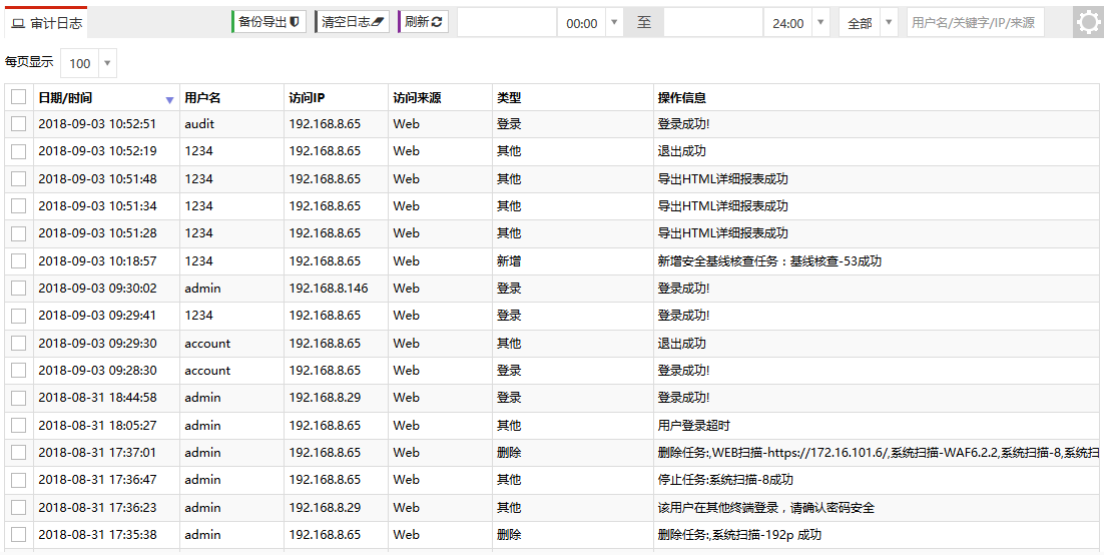
导出报表将实时显示导出进度，便于用户了解导出实时情况.

图8-4 导出扫描报表进度条显示

8.4 审计日志

审计日志以分页形式显示管理员对漏洞扫描系统所进行的操作管理记录，操作管理不仅包含 WEB 管理界面下的操作，还包括命令行管理界面下的操作，同时操作日志支持按条件的高级查询功能。

图8-5 审计日志



日期/时间	用户名	访问IP	访问来源	类型	操作信息
2018-09-03 10:52:51	audit	192.168.8.65	Web	登录	登录成功!
2018-09-03 10:52:19	1234	192.168.8.65	Web	其他	退出成功
2018-09-03 10:51:48	1234	192.168.8.65	Web	其他	导出HTML详细报表成功
2018-09-03 10:51:34	1234	192.168.8.65	Web	其他	导出HTML详细报表成功
2018-09-03 10:51:28	1234	192.168.8.65	Web	其他	导出HTML详细报表成功
2018-09-03 10:18:57	1234	192.168.8.65	Web	新增	新增安全基线核查任务：基线核查-53成功
2018-09-03 09:30:02	admin	192.168.8.146	Web	登录	登录成功!
2018-09-03 09:29:41	1234	192.168.8.65	Web	登录	登录成功!
2018-09-03 09:29:30	account	192.168.8.65	Web	其他	退出成功
2018-09-03 09:28:30	account	192.168.8.65	Web	登录	登录成功!
2018-08-31 18:44:58	admin	192.168.8.29	Web	登录	登录成功!
2018-08-31 18:05:27	admin	192.168.8.65	Web	其他	用户登录超时
2018-08-31 17:37:01	admin	192.168.8.65	Web	删除	删除任务:,WEB扫描-https://172.16.101.6/,系统扫描-WAF6.2.2,系统扫描-8,系统扫
2018-08-31 17:36:47	admin	192.168.8.65	Web	其他	停止任务:系统扫描-8成功
2018-08-31 17:36:23	admin	192.168.8.29	Web	其他	该用户在其他终端登录，请确认密码安全
2018-08-31 17:35:38	admin	192.168.8.65	Web	删除	删除任务:,系统扫描-192p 成功

9 快速向导

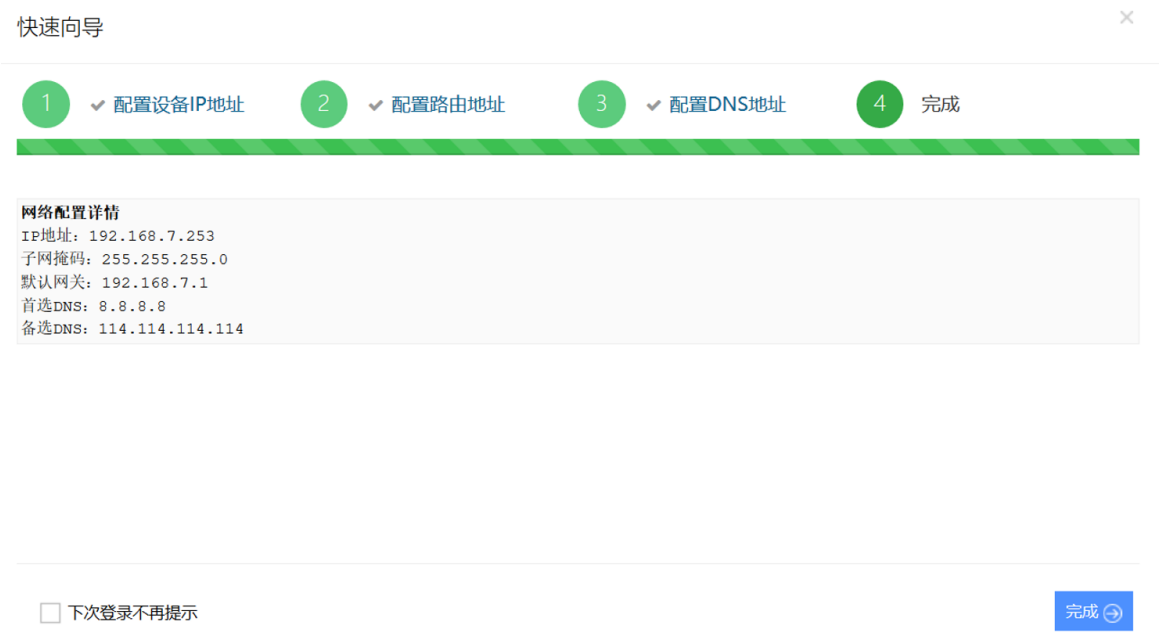
可以在快速向导界面按照步骤依次对设备 IP、设备路由、DNS 地址进行配置。

图9-1 配置设备 IP 地址

图9-2 配置路由地址

图9-3 配置 DNS 地址

图9-4 完成



10 出厂参数

表10-1 通讯设置

参数	说明
IP	默认所有接口的出厂地址为192.168.0.1
访问端口	443
网络掩码	255.255.255.0

表10-2 管理网口初始设置

参数	说明
波特率	9600
传输位数	8
奇偶校验	无
停止位	1
数据流控制	无