瑞和云图
Safe in Cloud

云翼-安全一体机系统
用户手册

北京瑞和云图科技有限公司

www.rivercloud.com.cn

2020 年

目录

版权申明

1.软件入门

1.1. 使用说明

如果您的访问业务较大，或者需要支持更多资产的扫描，可以联系开发厂商使用分布式部署方式。

1.2. 系统使用

将该系统接入网络后，打开浏览器（建议使用 chrome、firefox 或 ie10 及以上版本），输入地址：https://ip 即可访问综合扫描系统。

第一次进入系统会提示缺少许可文件，根据操作界面(下图)，复制授权号，把授权号发送给软件开发商，软件开发商会根据约定生成 license.dat，最后通过界面把 license.dat 文件导入系统即可。license.dat 许可文件只适用于指定的机器运行才有效，即授权号与 license.dat 是一对一关系。

2.操作入门

2.1. 用户登录

输入正确的用户名、密码、验证码后点击登录按钮，即可成功登录到系统。

- **首次登录系统会有 4 个默认的用户。（用户名分别为：admin、audit、secret、scan ，密码均为：用户名 123456）输入正确的验证码后即可登录，且该用户不能被删除和锁定。**
- **创建的用户密码输入错误 5 次会被锁定 300 秒，可通过系统管理菜单里的用户管理进行解锁。（可在用户管理中对密码输入的错误次数和锁定时间进行设置）**

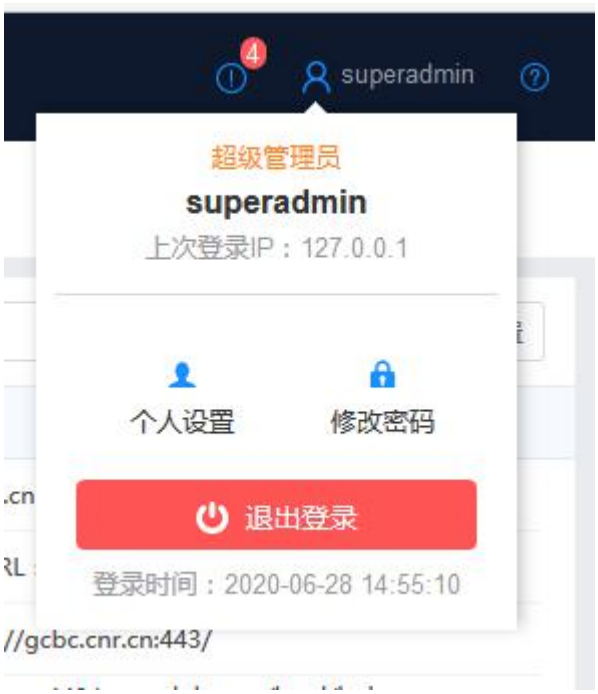
3.管理界面

3.1. 预警提示

页面右上角：预警提示，显示弱点总条数，可点击查看预警详情（风险类型、名称和预警时间）。

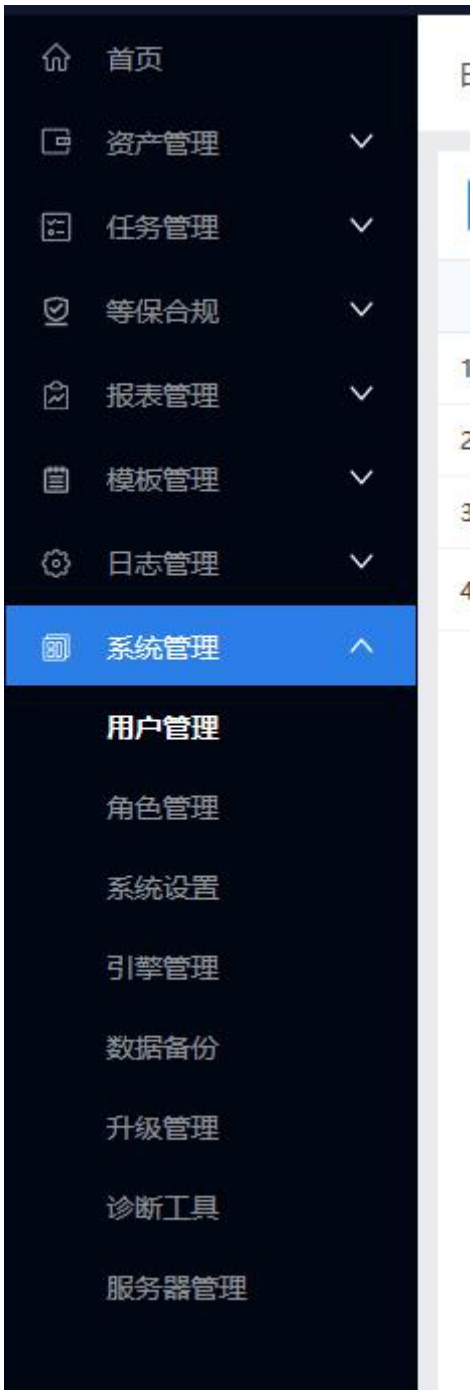
3.2. 用户信息

页面右上角：用户信息，显示当前用户，可以查看用户名、角色、登录时间、上次登录 IP，还可以修改当前用户密码和切换用户。



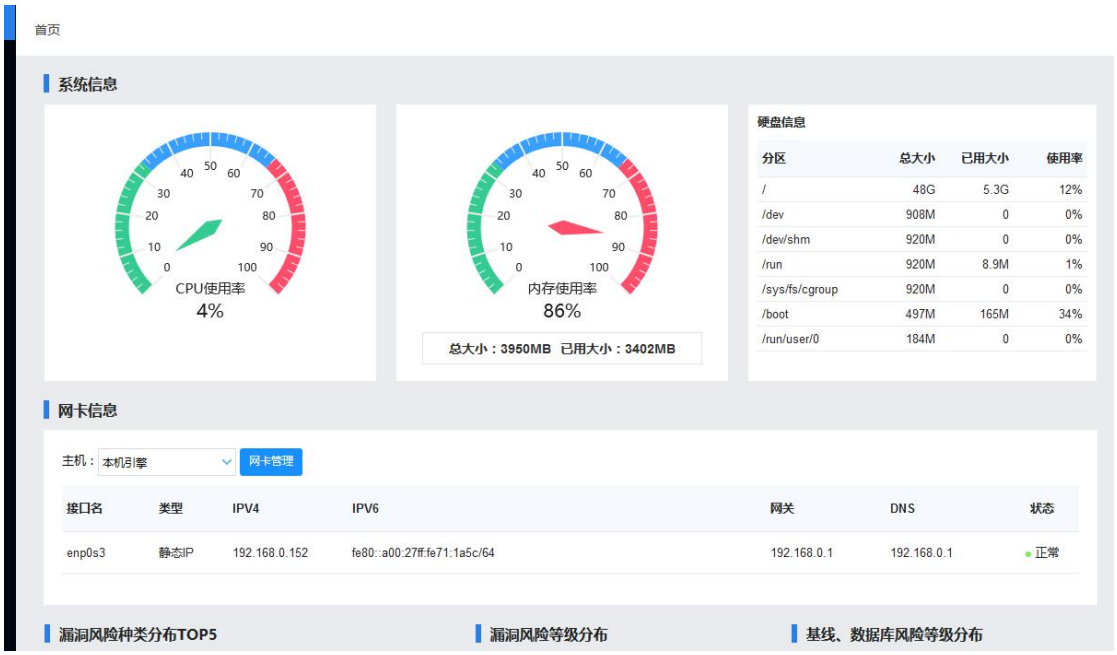
4.菜单

不同的用户登录可能看见的菜单不同，系统只会显示当前登录用户有权限的菜单。



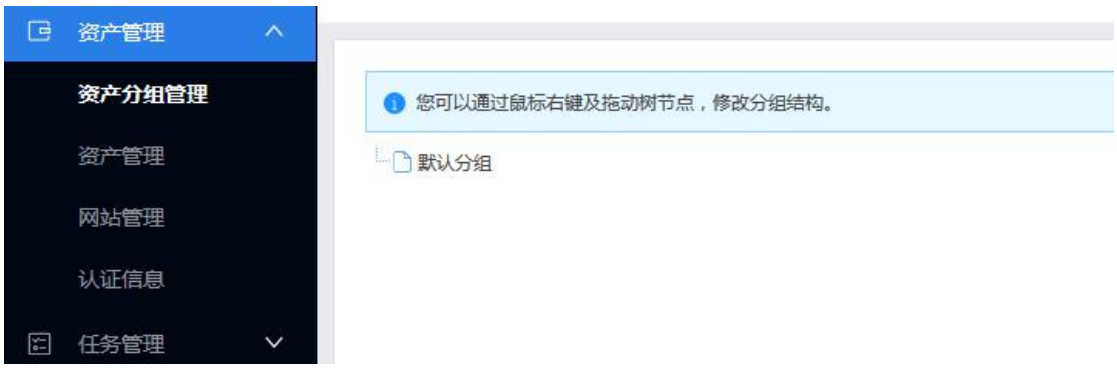
4.1. 首页菜单

该页面主要用于显示系统使用状态以及风险状态。



4.2. 资产管理菜单

资产管理菜单包括资产分组管理、资产管理、网站管理和认证信息。



4.2.1. 资产分组管理

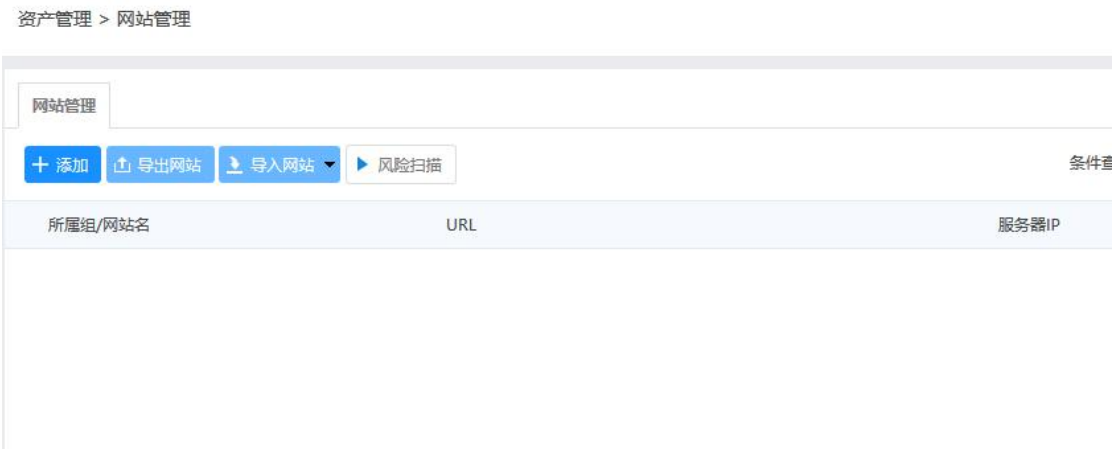
该模块主要用于管理平台的所有资产组，便于对资产做管理以树的形式显示资产组，支持无限极管理资产组。资产组位于资产管理左侧。

4.2.2. 资产管理

该模块主要用于管理平台所有资产，便于在添加任务的时候选择资产。以列表的方式显示资产名称、资产类型、所属区域、描述等信息。资产管理主要分为“资产组”和“资产列表”，创建资产时需先选择资产。

4.2.3. 网站管理

该模块主要用于管理平台所有网站资产，便于在添加网站任务的时候选择资产。以列表的方式显示资产名称、资产类型、所属区域、描述等信息。资产管理主要分为“资产组”和“资产列表”，创建资产时需先选择资产。



4.2.4. 认证信息

该模块主要用于管理资产的认证信息，个别扫描功能在对资产进行安全评估时需要使用用户名及密码等信息登录目标资产，这里主要用于管理资产对应的登录方式。

4.3. 任务管理菜单

任务管理菜单包括资产梳理、主机漏洞扫描、基线配置核查、网站漏洞监控、网站篡改监测、网站可用性监测、数据库漏洞扫描、弱口令猜解等。

4.3.1.资产梳理

根据探测目标、探测端口范围等参数信息自动发现目标网络中的资产。

4.3.2. 主机漏洞扫描

4.3.2.1. 任务管理

该模块主要用于管理平台所建的主机漏洞扫描任务。以列表的方式显示任务名称、扫描周期、预警方式、预警周期、当前状态等信息。

- **点击**  **按钮，输入信息，即可添加扫描任务；**

■ **点击** **按钮，即可查看任务详情；**

4.3.3.基线配置核查

该模块主要用于管理平台所建的基线扫描任务。以列表的方式显示任务名称、扫描类型、预警方式、告警类型、任务状态等信息。

- **点击** 

按钮，输入信息，即可添加扫描任务；

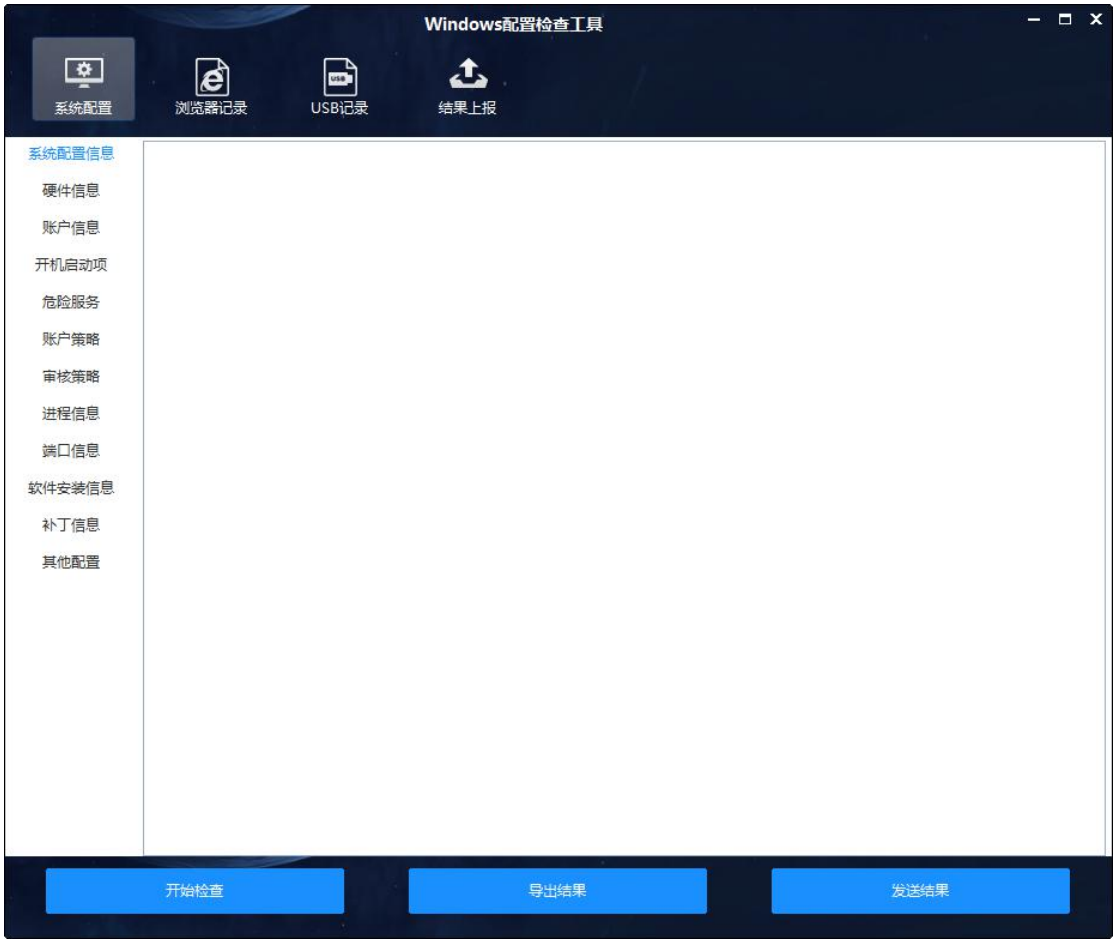
- **点击** 

按钮，选择文件，即可上报离线扫描结果；

- **点击** 

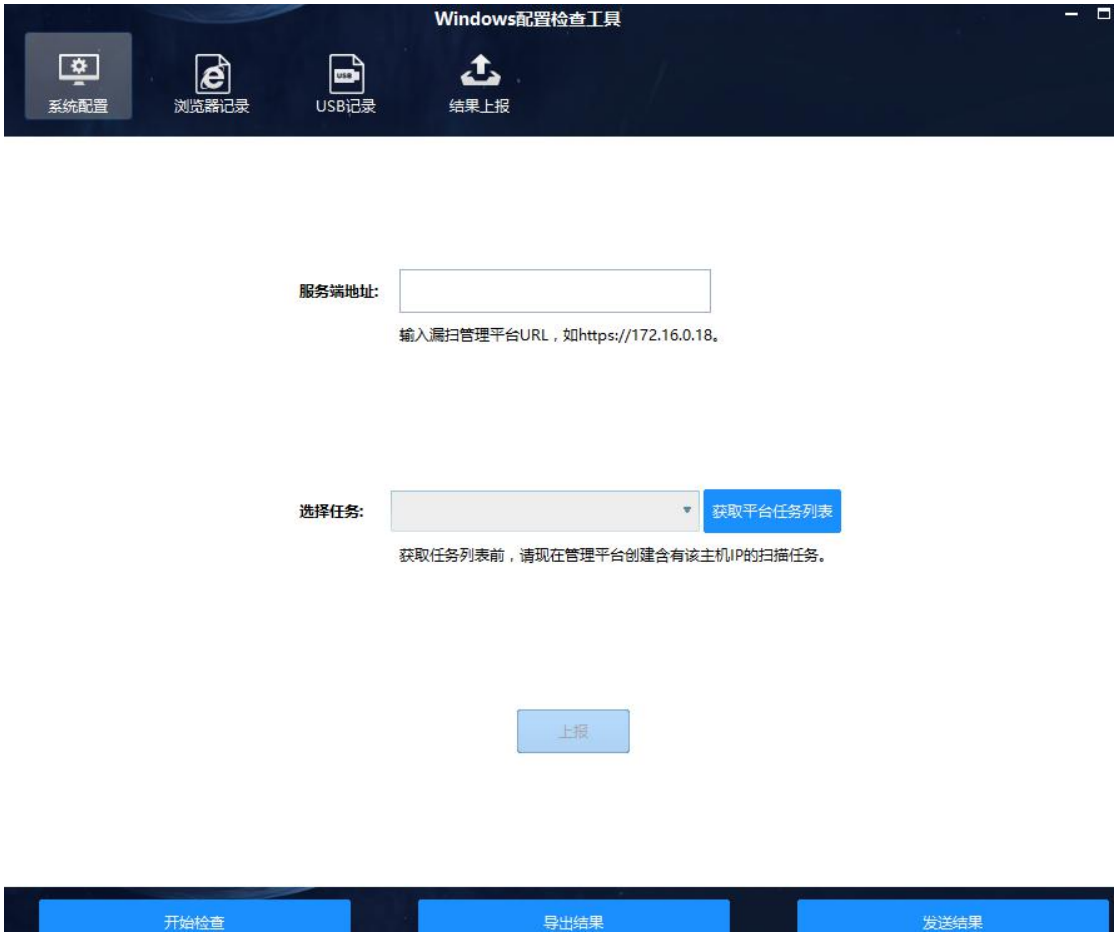
按钮，即可下载 Windows 离线检查工具

(Windows 离线检查工具即检查本机的配置核查)



点击“开始扫描”即可扫描本机的配置，扫描完成后可“自动上报”也可“导出结果”。

自动上报：输入服务端地址和选择任务即可上报。



4.3.4. 网站漏洞监控

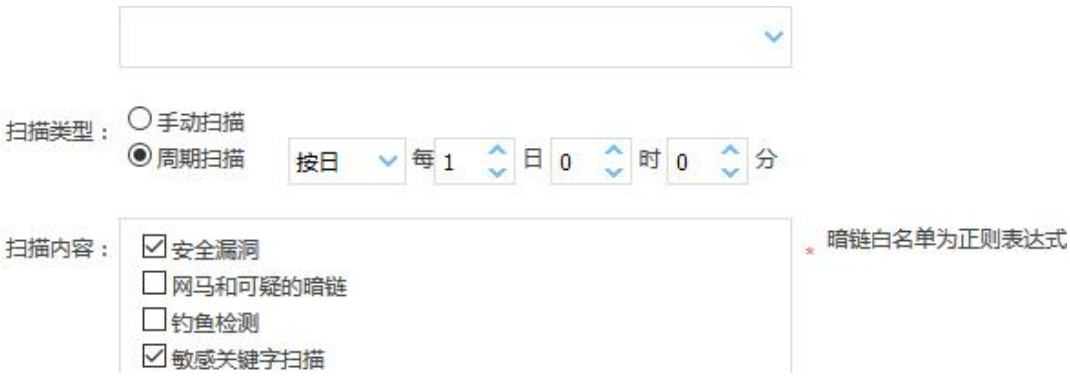
该模块主要用于管理平台所建的网站监控任务。网站安全监控主要对目标网站的可用性、安全漏洞、篡改、网马、暗链等进行 7*24 小时监控，也可对安全漏洞进行单次评估扫描。全面支持 OWASP TOP 10 2013 漏洞检测，如 SQL 注入、跨站脚本、文件包含、命令执行、信息泄漏等全部漏洞；覆盖了论坛、内容管理系统（CMS）和电子商务应用系统等平台。

4.3.4.1. 单次扫描

对目标网站进行单次扫描，可扫描网站的漏洞。

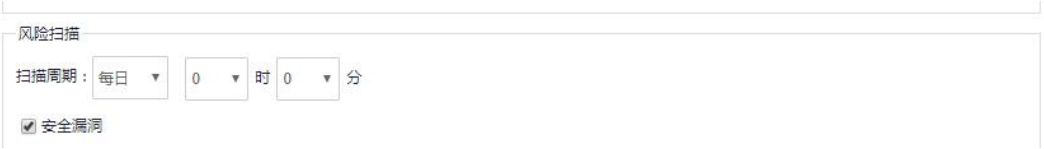
4.3.4.2. 周期扫描

对目标网站进行周期性监控，包括安全漏洞、网马和暗链、敏感内容等。



4.3.4.2.1. 安全漏洞

安全漏洞包括 SQL 注入漏洞、SQL 盲注漏洞、XPath 注入漏洞、XSS 跨站脚本漏洞、目录遍历漏洞、源代码泄露漏洞等。



4.3.4.2.2. 网马和暗链

网页挂马是攻击者通过在正常的页面中（通常是网站的主页）插入一段代码。浏览者在打开该页面的时候，这段代码被执行，然后下载并运行某木马的服务器端程序，进而控制浏览者的主机。通俗点说就是将网页木马这样的攻击程序放在网页上，浏览这个网页的人，不需要任何点击动作就会中毒。

常见的网页挂马实现方式：

1) iframe 框架嵌入式挂马

2) JS 文件调用挂马

3) JS 文件加密变形

4) JavaScript 脚本挂马

5) Body 挂马等。

“暗链”就是看不见的网站链接，“暗链”在网站中的链接做得非常隐蔽，短时间内不易被搜索引擎察觉。它和友情链接有相似之处，可以有效地提高 PR 值。但要注意一点 PR 值是对单独页面，而不是整个网站。

如果网站被挂马或被写入暗链，对于网站的运营来说是非常不利的，他会影响搜索引擎的排名、被降权，同时网站的数据也有可能被泄露。同时，还会篡改网站标题、网站内容，

添加大量垃圾链接，导致网站面目全非。因此，解决网站被挂马问题、暗链问题是必要的。

4.3.4.2.3. 敏感内容

网站如果被篡改，在网站页面添加了一些带有敏感政治倾向（或反执政党倾向）、暴力倾向、不健康色彩的词或不文明语、博彩等的敏感内容，将影响企业的品牌形象，严重的可能照成经济损失。

4.3.4.3. 扫描参数

4.3.4.3.1. 基本配置

4.3.5.网站可用性监测

该模块主要用于管理平台所建的网站可用性监测任务。网站可用性监测主要对目标网站的可用性进行 7*24 小时监控。

4.3.6. 网站篡改监测

该模块主要用于管理平台所建的网站篡改监测任务。网站篡改监测主要对目标网站的篡改性进行 7*24 小时监控，包括：内容篡改、图片篡改、新增 URL、删除 URL。

4.3.7. 数据库扫描

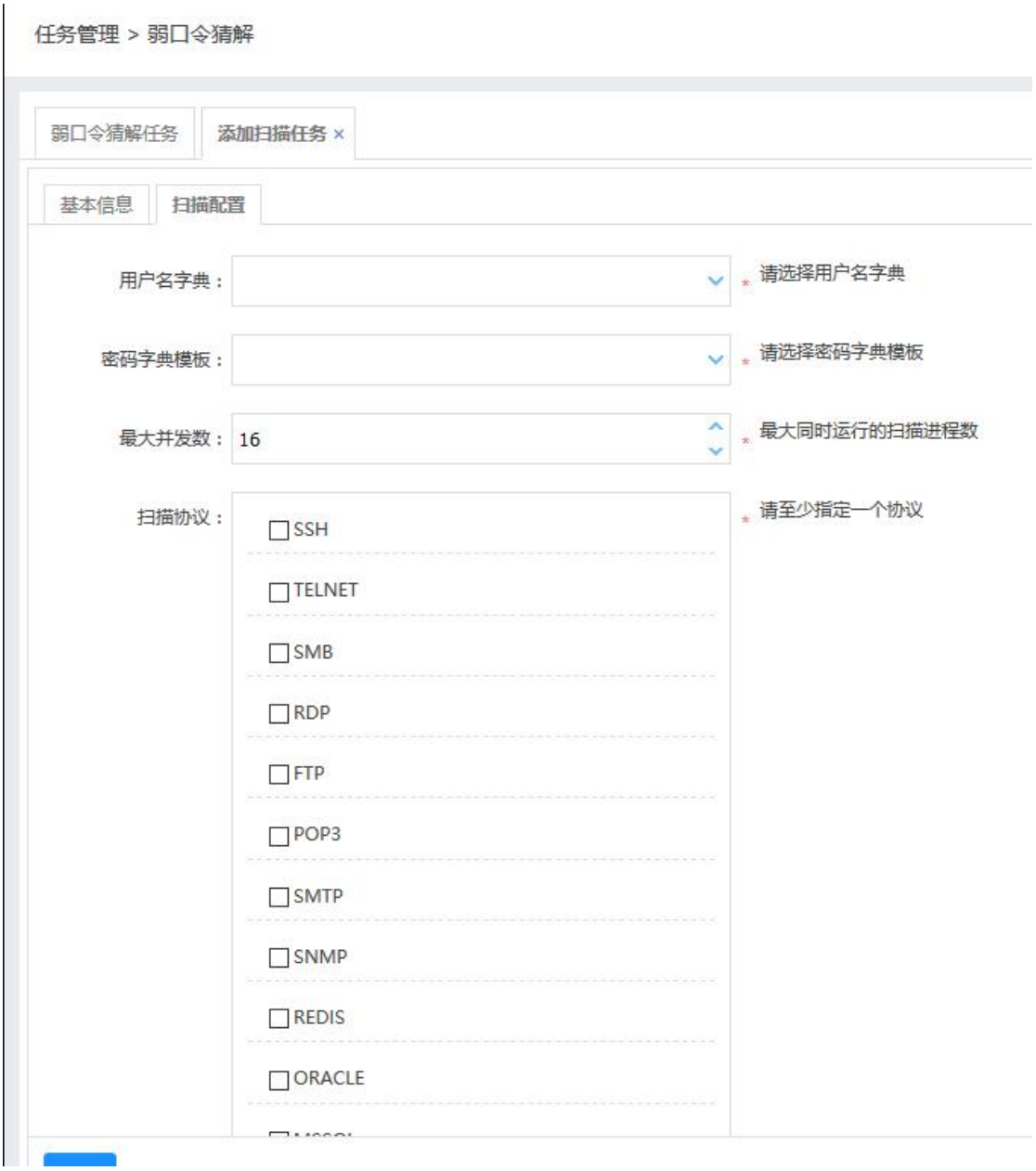
该模块主要用于管理平台所建的数据库扫描任务。以列表的方式显示任务名称、扫描类型、告警方式、告警类型、当前状态以及对任务的描述等信息。

■ **点击**  **按钮，输入信息，即可添加扫描任务；**

4.3.8.弱口令猜解

该模块主要用于管理平台所建的弱口令扫描任务。以列表的方式显示任务名称、扫描类型、告警方式、告警类型、当前状态以及对任务的描述等信息。

- **点击**  **按钮，输入信息，即可添加扫描任务；**



扫描协议选择（根据目标开启的服务开选择协议）：

SSH：目标开启了 SSH 服务，如 LINUX 系统、网络设备、安全设备等。

TELNET：目标开启了 TELNET 服务，如 LINUX 系统、网络设备、安全设备等。

SMB/RDP：目标为 WINDOWS 操作系统。

FTP：目标开启了 FTP 服务。

POP3/SMTP：目标为邮件服务器。

SNMP：目标开启了 SNMP 服务，如服务器、网络设备、安全设备等。

REDID/ORACLE/MSSQL/MYSQL/POSTGRES/：目标安装了对应的数据库服务。

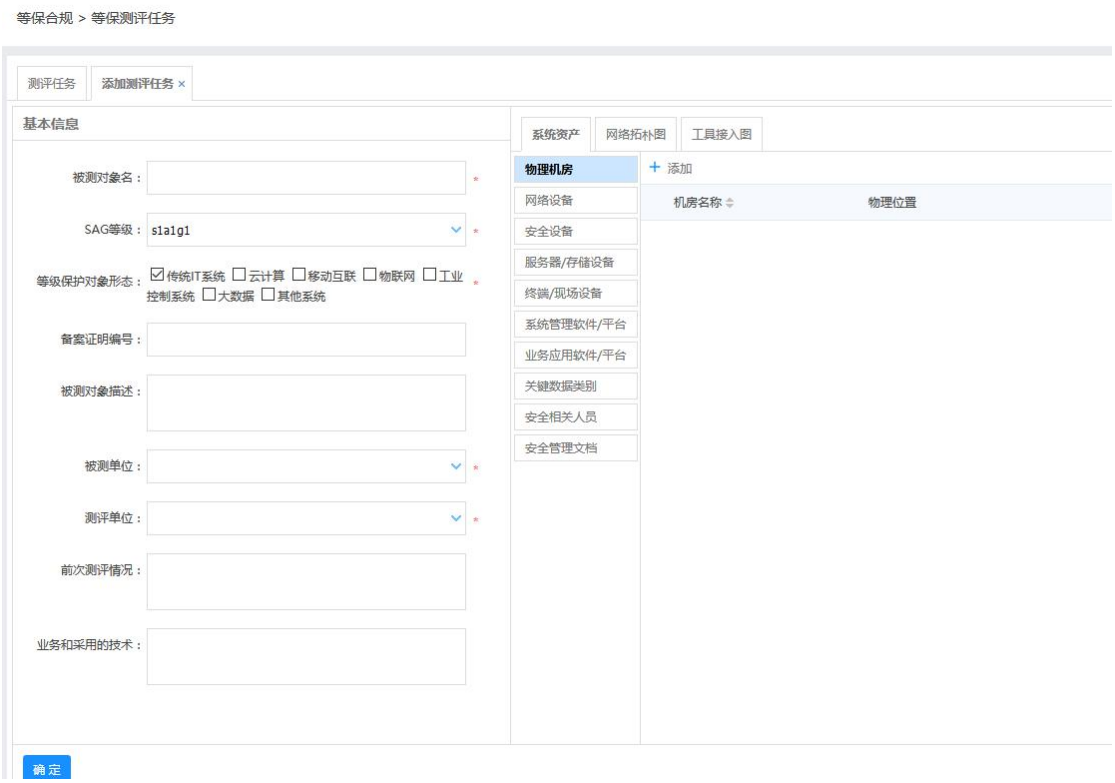
HTTP：目标为 WEB 服务器，且登陆页面没有验证码。

4.4. 等保合规菜单

该模块主要用于管理平台所建的信息系统测评任务。以列表的方式显示信息系统名称、被测单位名称、系统简介、SAG 等级、资产数等信息。

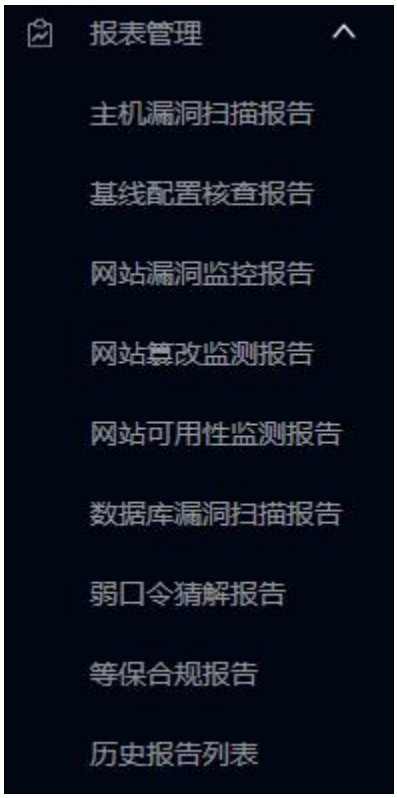
- **点击** 

按钮，输入信息，即可添加信息系统测评任务；



4.5. 报表管理菜单

报表管理菜单包括主机漏洞扫描报告、基线配置核查报告、网站漏洞监控报告、网站篡改监测报告、网站可用性监测报告、数据库漏洞扫描报告、弱口令猜解报告等。



4.5.1.主机漏洞扫描报告

选择相应的任务，可修改报告名称，点击 预览 按钮，即可预览报告详情；

4.5.2.基线配置核查报告

选择相应的任务，可修改报告名称，点击 预览 按钮，即可预览报告详情；

4.5.3.网站漏洞监控报告

选择相应的任务，可修改报告名称，点击 

按钮，即可预览报告详情；

4.5.4. 网站篡改监测报告

选择相应的任务，可修改报告名称，点击 

按钮，即可预览报告详情；

4.5.5.网站可用性监测报告

选择相应的任务，可修改报告名称，点击 

按钮，即可预览报告详情；

4.5.6.数据库漏洞扫描报告

选择相应的任务，可修改报告名称，点击 

按钮，即可预览报告详情；

4.5.7.弱口令猜解报告

选择相应的任务，可修改报告名称，点击 

按钮，即可预览报告详情；

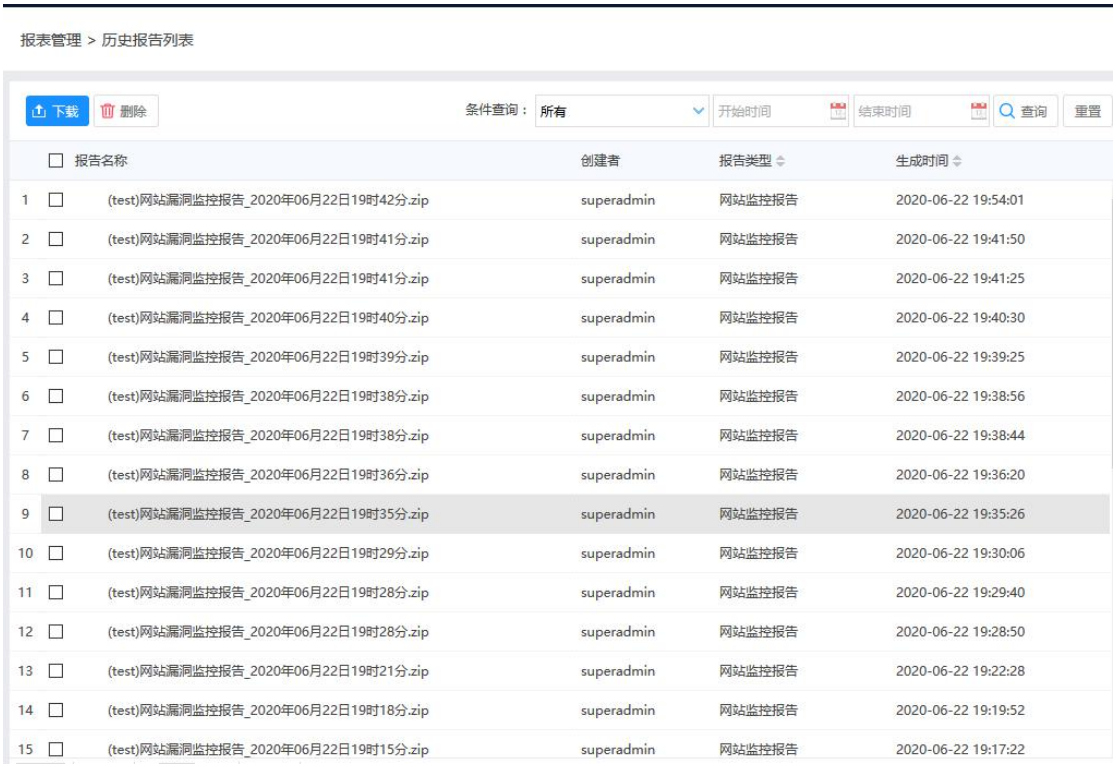
4.5.8.等保合规报告

选择相应的任务，可修改报告名称，点击 

按钮，即可预览报告详情；

4.5.9..历史报告列表

该模块主要用于管理以前所有已经导出的报告，方便用户追踪查看历史监控情况。已列表的方式显示报告名称、生成时间、报告类型等内容。可批量导出报告。

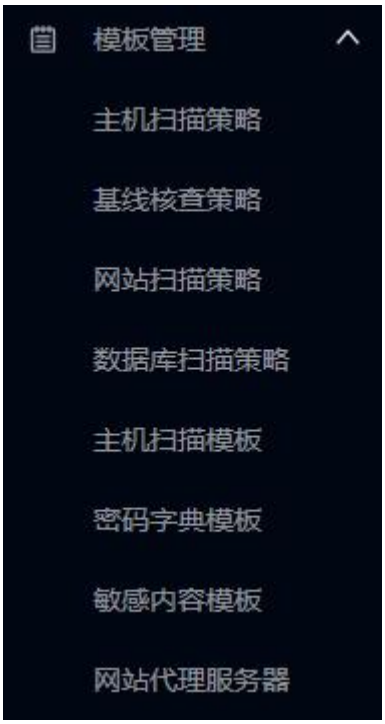


- **勾选需要导出的报告，点击工具栏中的** 

按钮，即可批量下载报告；

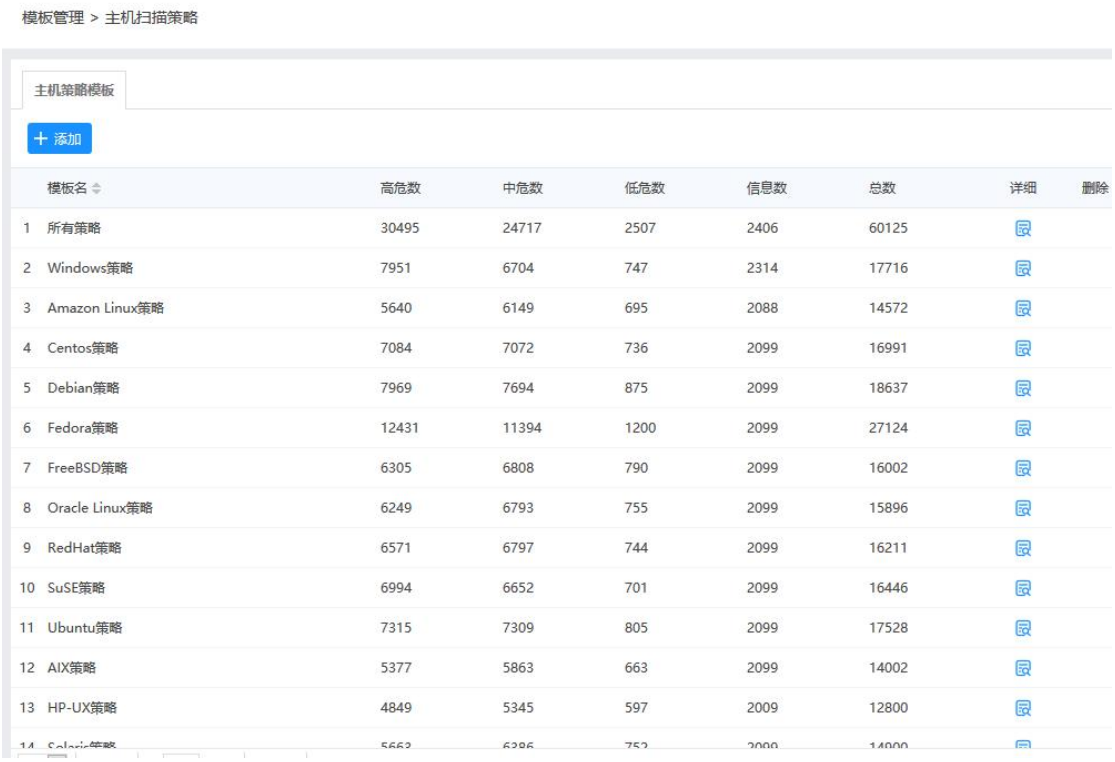
4.6. 模板管理菜单

模板管理菜单包括主机扫描策略、基线核查策略、网站扫描策略等。



4.6.1.主机扫描策略

该模块的主要功能为将常用的主机扫描策略保存起来，方便直接应用到各个不同的主机扫描任务中，以列表的方式显示模板名称和配置内容等信息。（默认的策略模板不可修改、删除）

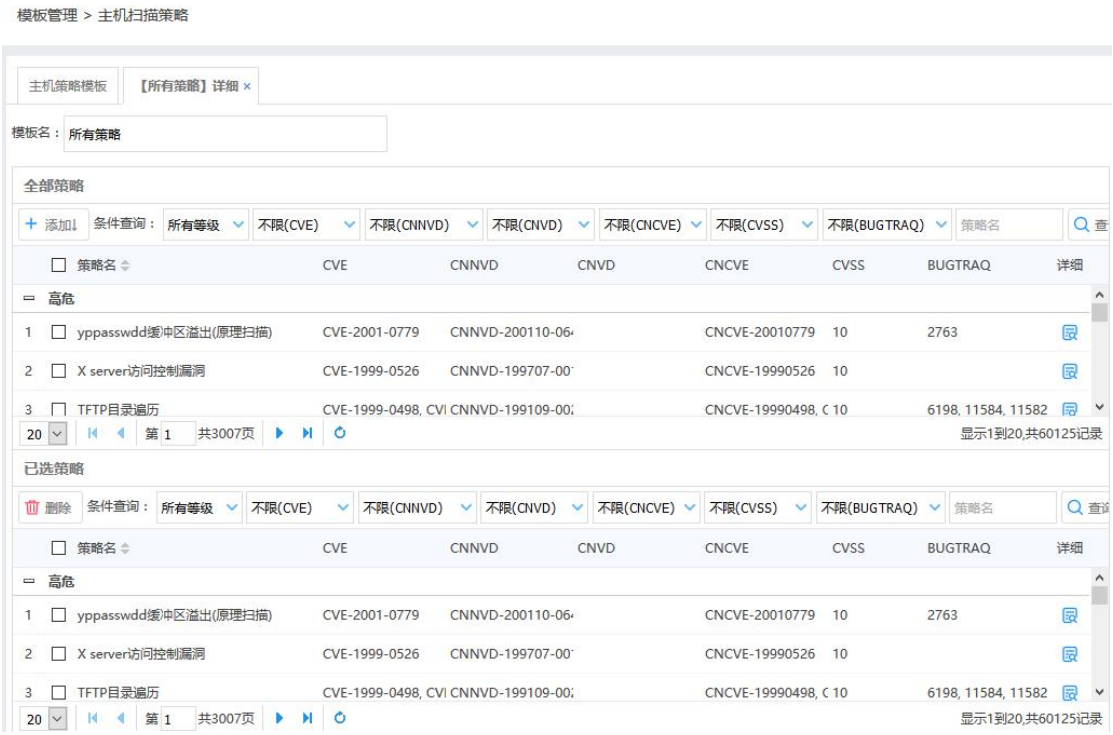


	模板名	高危数	中危数	低危数	信息数	总数	详细	删除
1	所有策略	30495	24717	2507	2406	60125		
2	Windows策略	7951	6704	747	2314	17716		
3	Amazon Linux策略	5640	6149	695	2088	14572		
4	Centos策略	7084	7072	736	2099	16991		
5	Debian策略	7969	7694	875	2099	18637		
6	Fedora策略	12431	11394	1200	2099	27124		
7	FreeBSD策略	6305	6808	790	2099	16002		
8	Oracle Linux策略	6249	6793	755	2099	15896		
9	RedHat策略	6571	6797	744	2099	16211		
10	SuSE策略	6994	6652	701	2099	16446		
11	Ubuntu策略	7315	7309	805	2099	17528		
12	AIX策略	5377	5863	663	2099	14002		
13	HP-UX策略	4849	5345	597	2009	12800		

■ **点击工具栏中的**  **按钮，即可添加策略模板；**

直接输入模板名添加；

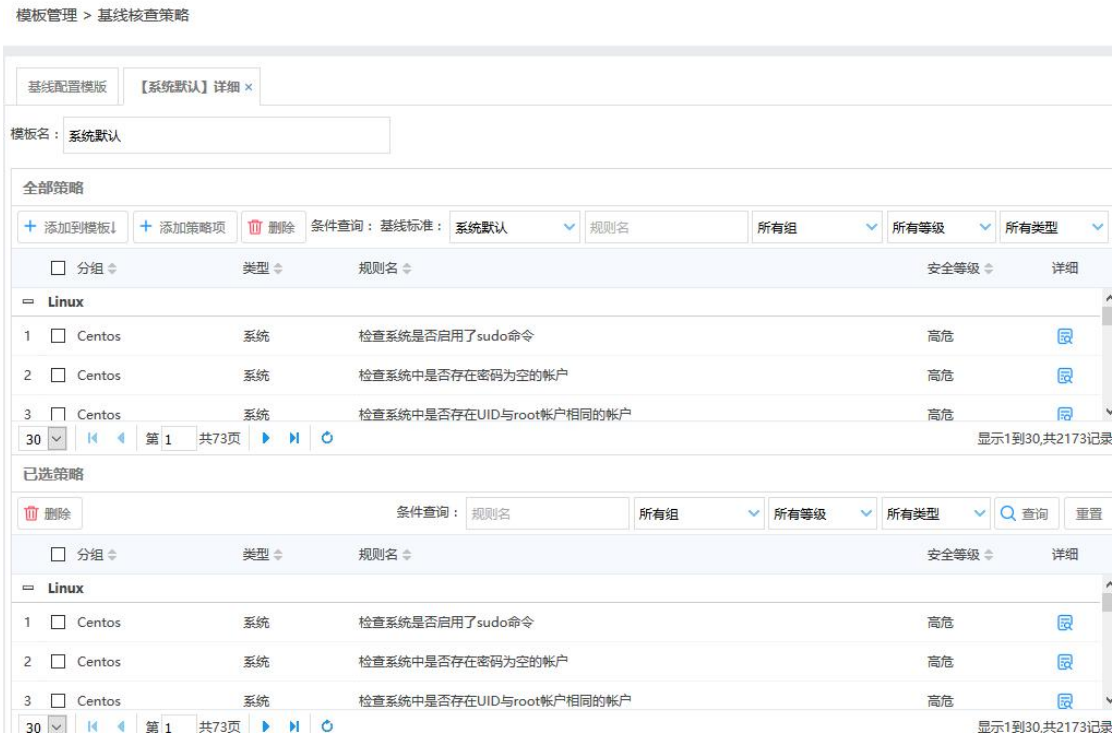
也可勾选系统中的策略进行添加；



4.6.2. 基线核查策略

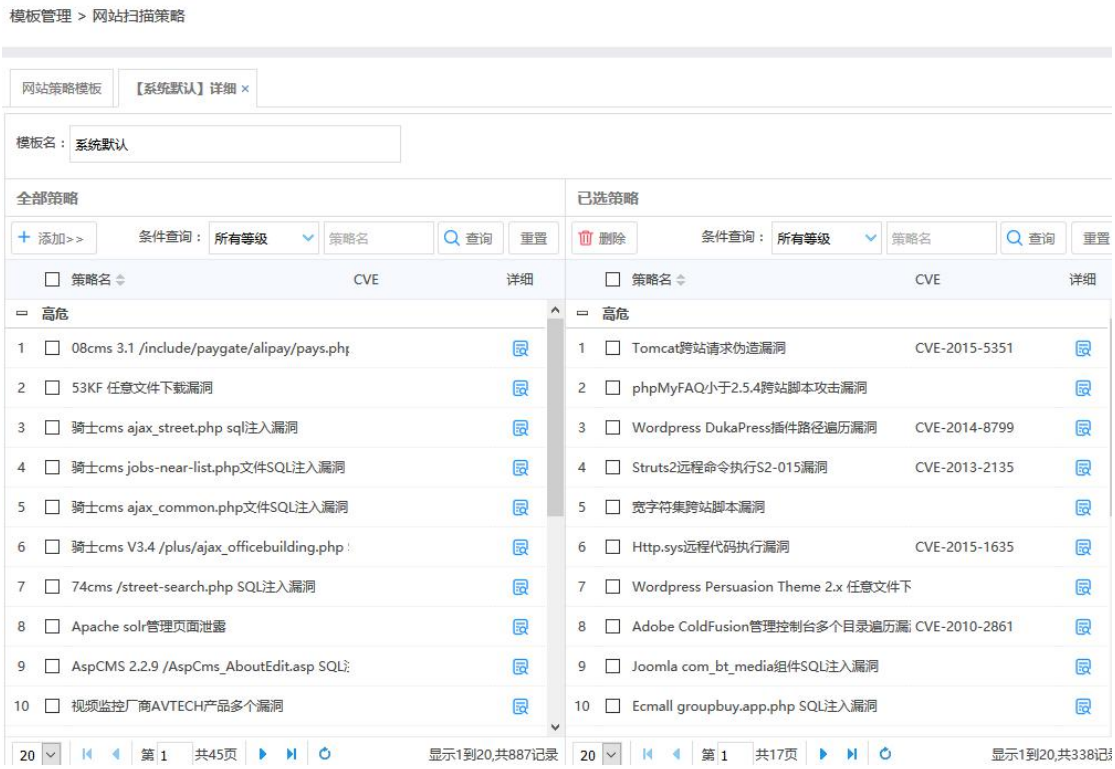
该模块以列表的方式显示模板名称、所属分组和策略总数等信息。（基线评估模板不可添加、修改、删除）

- **点击 按钮，即可查看模板的详情，以列表的方式显示策略名称、等级、检查点、检查项、所属策略模板、所属策略分组等信息；**



4.6.3.网站扫描策略

该模块的主要功能是添加、删除网站策略模版，也可查看全部的网站扫描策略，支持对策略进行检索。



4.6.4..数据库扫描策略

该模块的主要功能是管理数据库策略，以列表的方式显示模板名称、紧急、高危、中危、低危、信息策略数等信息。（数据库策略模板不可添加、修改、删除）

4.6.5.敏感关键字模板

该模块的主要功能是添加、删除网站安全监控中的敏感关键字。

4.6.6.网站代理服务器

该模块的主要功能的添加、删除访问的网站代理服务器。可导入和导出服务器模板。

4.6.7.密码字典模板

该模块的主要功能为将常用的弱口令字典保存起来，方便直接应用到各个不同的弱口令扫描任务中，以列表的方式显示字典名称、字典类型和字典内容等信息。（系统默认的弱口令字典不可修改、删除）

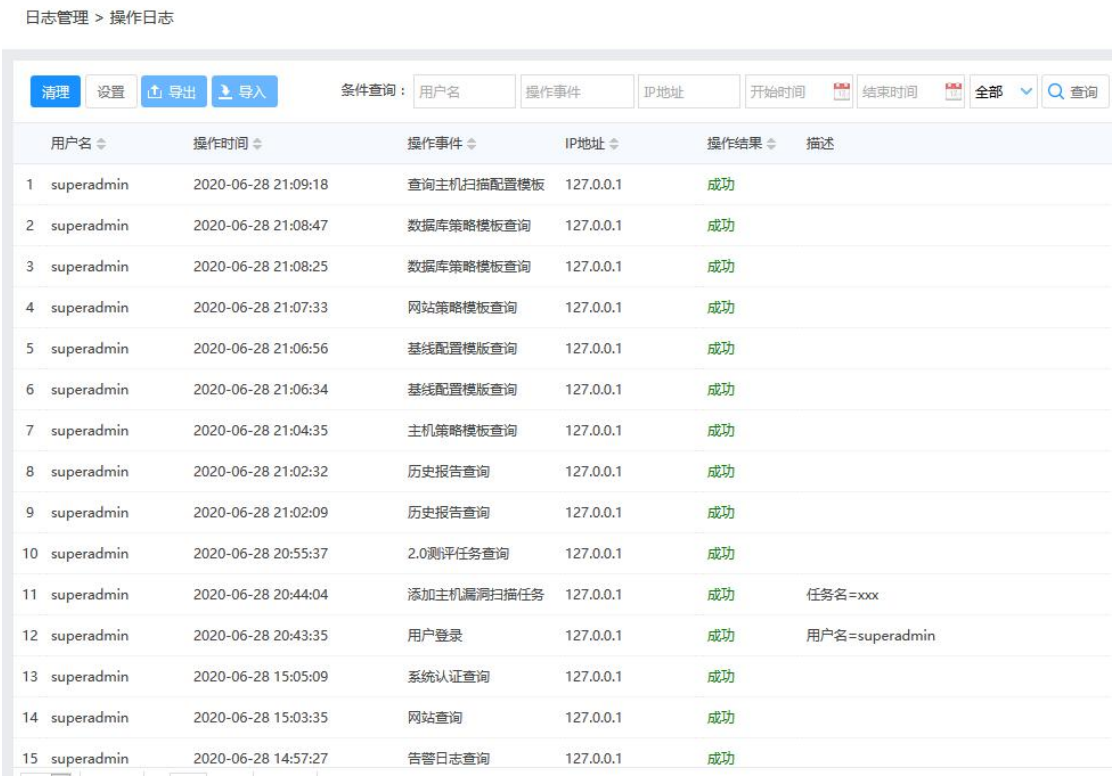
	字典名	字典类型	内容	字典描述	字典文件	修改
1	SSH账号字典	用户名字典			sshuser.txt	
2	SSH账号字典_大字典	用户名字典			sshuserbig.txt	
3	SSH密码字典	密码字典			sshpass.txt	
4	SSH密码字典 _ 大字典	密码字典			sshpassbig.txt	
5	snmp密码字典	密码字典			snmppass.txt	
6	SMB账户字典_大字典	用户名字典			smbuserbig.txt	
7	SMB账号字典	用户名字典			smbuser.txt	
8	SMB密码字典	密码字典			smbpass.txt	
9	SMB密码大字典	密码字典			smbpassbig.txt	
10	网络设备默认用户字典	用户名字典			netdevdefuser.txt	
11	网络设备默认密码字典	密码字典			netdevdefpass.txt	
12	密码字典	密码字典			password.txt	
13	用户名字典	用户名字典			username.txt	

4.7. 日志管理菜单

日志管理菜单包括操作日志、系统日志、告警日志。

4.7.1.操作日志

操作日志记录了用户对系统进行的所有操作，以列表的方式显示操作时间、操作用户、操作事件以及描述信息等。



4.7.2.系统日志

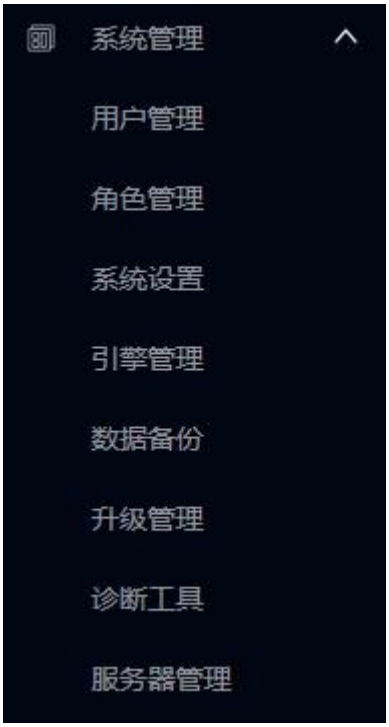
系统日志记录了系统自动进行的一系列操作，如定时任务、预警等。

4.7.3.告警日志

告警日志记录了系统的所有告警信息，如发现资产漏洞、系统资源使用率过高等。

4.8. 系统管理菜单

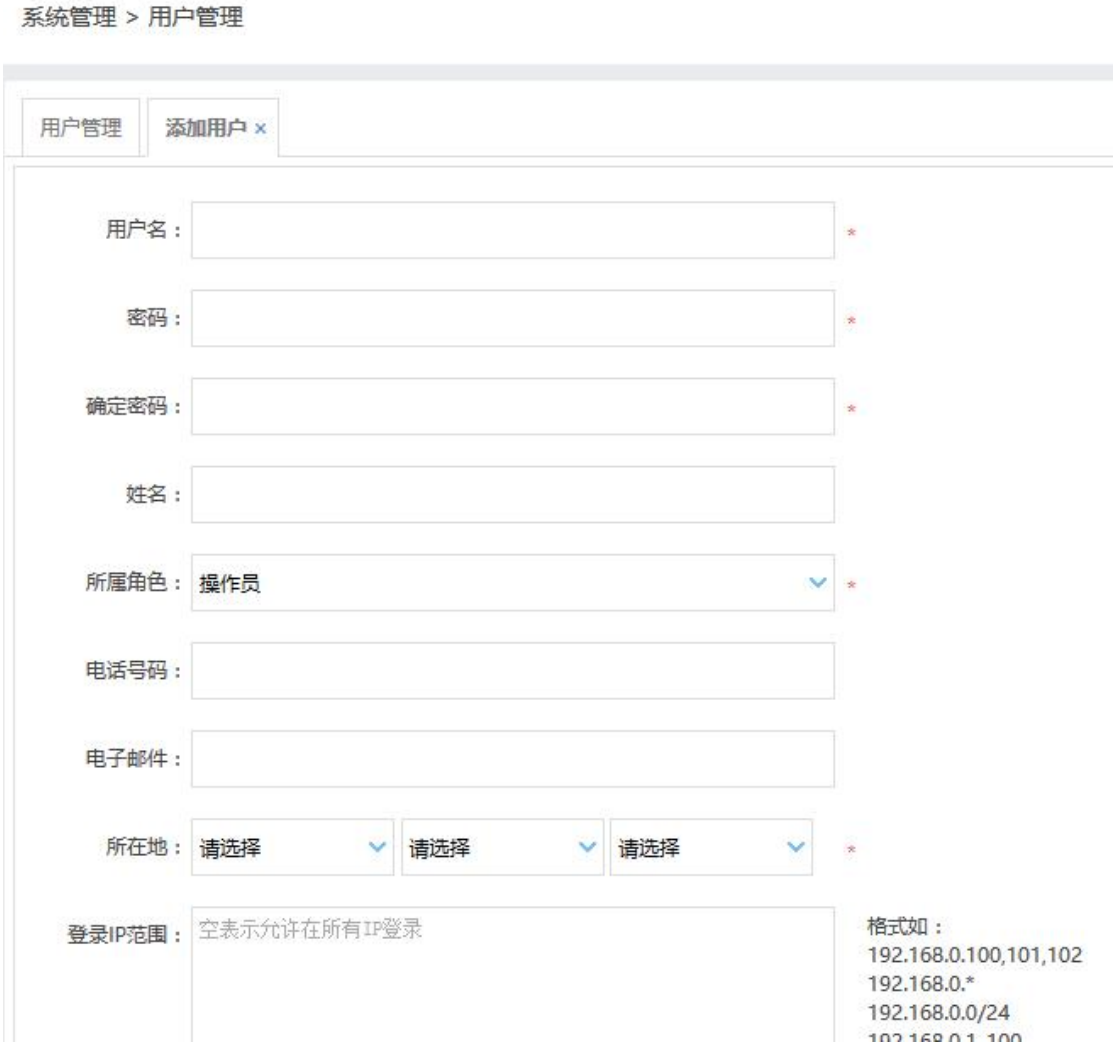
系统管理菜单包括用户管理、角色管理、系统设置、引擎管理、诊断工具等。



4.8.1. 用户管理

以列表的方式显示用户的详细信息，包括用户名、姓名、创建时间、所属角色、所属区域、最后登录时间、锁定状态和最后登录 IP 地址。（系统默认管理员不可修改、删除、锁定/解锁）

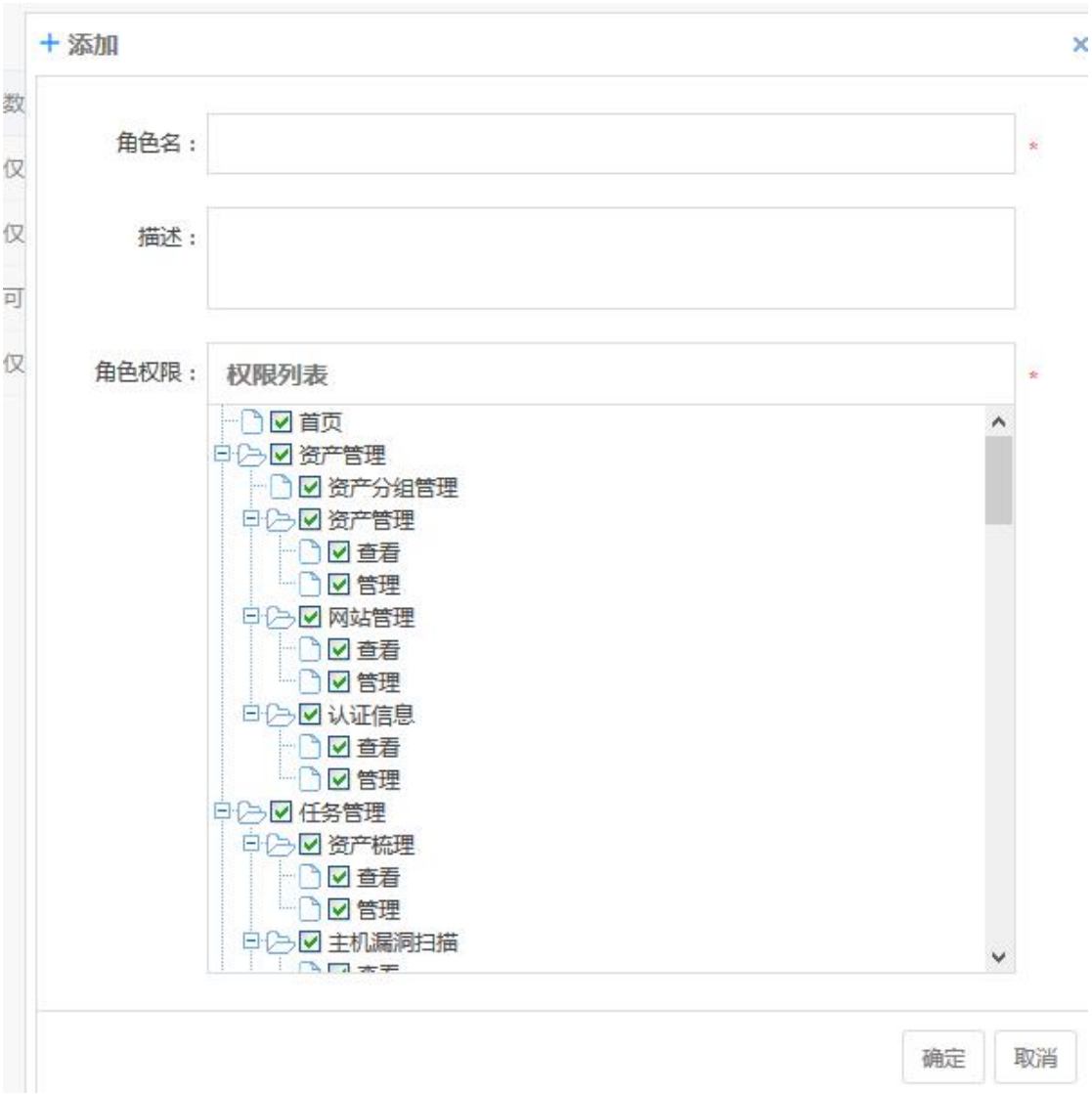
■ **点击**  **按钮，输入信息，即可添加用户；**



4.8.2.角色管理

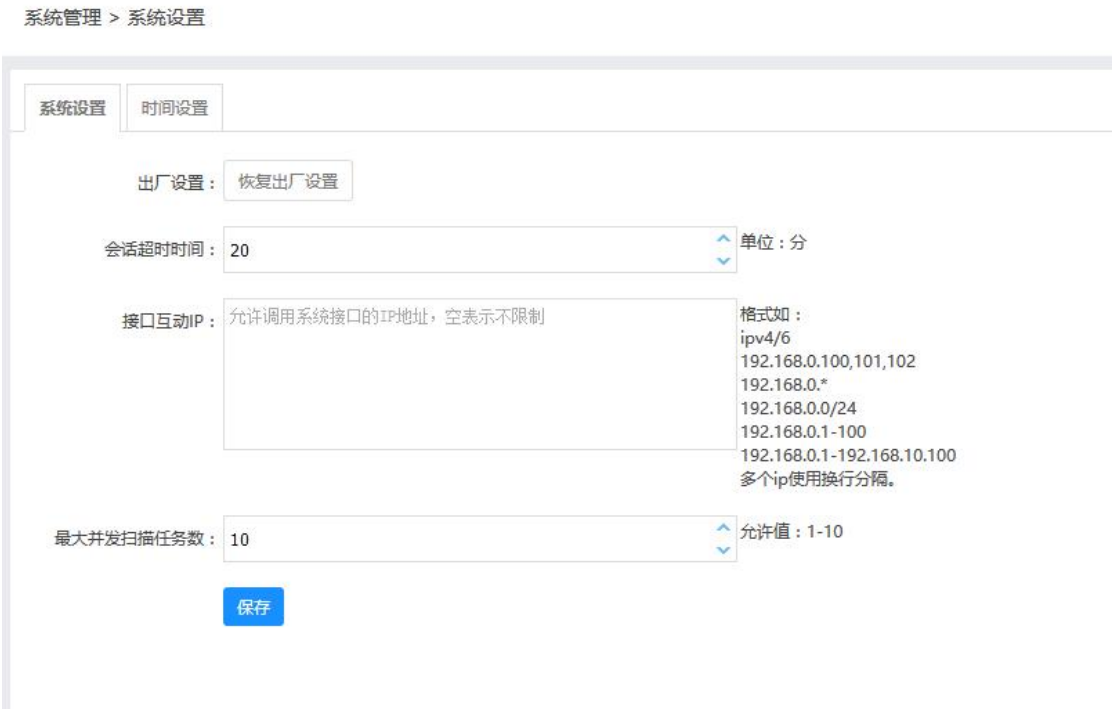
以列表的方式显示角色的详细信息，包括角色名、描述和权限。（系统默认管理员、审计员、操作员不可修改、删除）

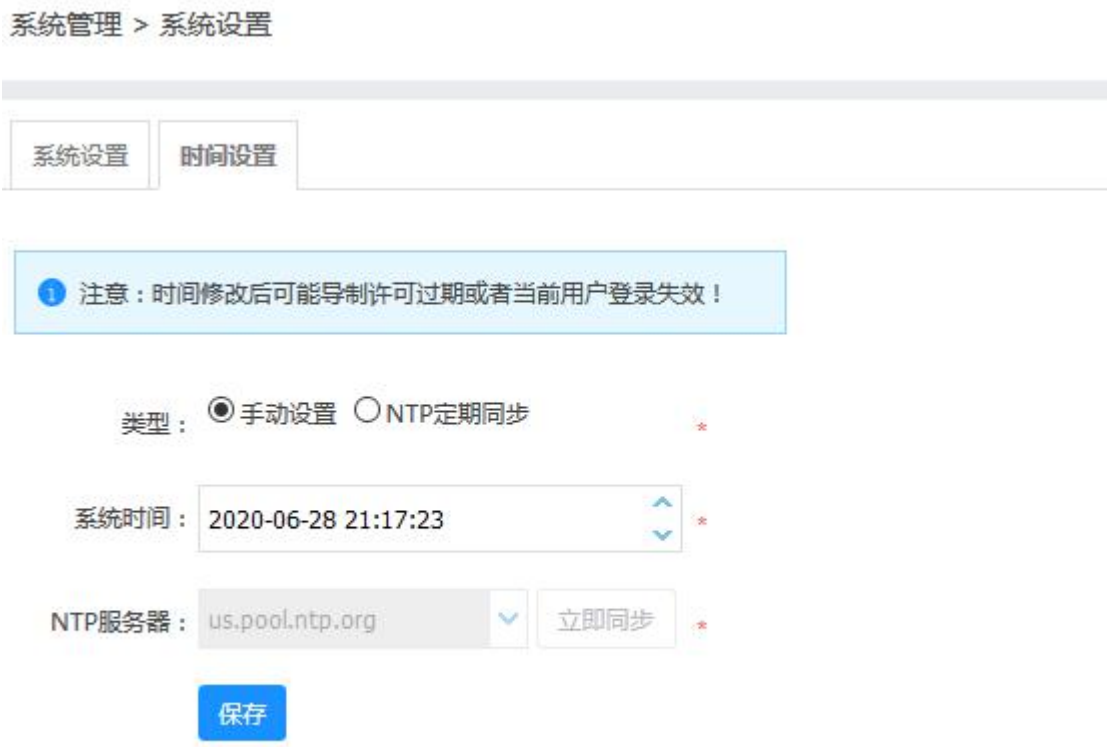
- **点击**  **按钮，输入信息，即可添加角色；**



4.8.3.系统设置

可对系统的会话超时时间、系统时间等进行设置。





4.8.4.引擎管理

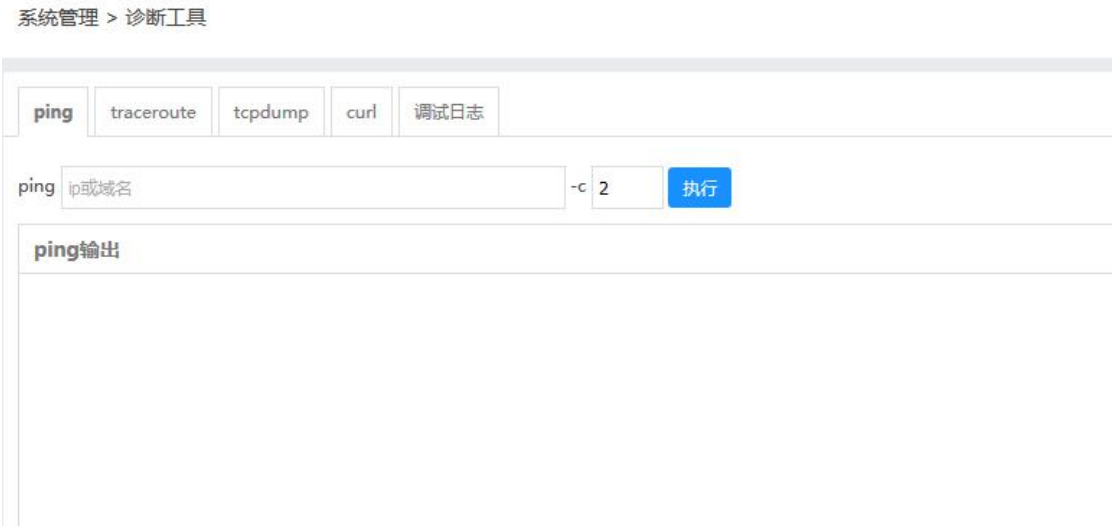
以列表方式显示所有扫描引擎，并能够查看引擎状态、接收的任务数等。

4.8.5.数据备份

用于对系统进行备份、恢复操作。

4.8.6.诊断工具

包含 ping、curl、traceroute 等常用工具，可用于系统网络诊断。



4.8.7.升级管理

用于对系统进行升级，包括离线升级、在线升级等。

4.8.8.服务器管理


系统管理 > 服务器管理
系统服务
预警邮件服务器
FTP服务器
SYSLOG服务器
WSUS联动
SSH服务：
关闭
SNMP服务：
关闭