

快页网站安全监测平台 (云网安) 用户手册

V1.0

KUAIYE 快页

快页

KUAIYE®

南京市大周路 32 号软件谷科创城 D2 南 8 楼 210012

版权声明

本手册中的所有内容及格式的版权属于快页公司（以下简称快页）所有，未经快页许可，任何人不得仿制、拷贝、转译或任意引用。

版权所有 不得翻印 ©2019 快页公司

商标声明

本手册中所谈及的产品名称仅做识别之用。手册中涉及的其他公司的注册商标或是版权属各商标注册人所有，恕不逐一列明。

KUAIYE®快页公司

目录

1	前言	1
1.1	文档目的	1
1.2	读者对象	1
1.3	文档基本内容	1
1.4	约定	2
1.5	相关文档	2
1.6	技术服务体系	2
2	系统简介	3
2.1	系统组成	3
2.2	系统功能	4
2.2.1	资产探测	4
2.2.2	内容检测	4
2.2.3	漏洞扫描	5
2.2.4	应用监控	5
2.2.5	告警管理	5
3	初次使用系统	6
3.1	系统登录	6
3.2	角色权限	7
4	普通用户	9
4.1	主页	9
4.2	资产中心	9
4.3	安全检测	10
4.3.1	资产探测	10
4.3.2	内容检测	12
4.3.3	漏洞扫描	16
4.3.4	应用监控	17
4.4	告警管理	17
4.4.1	告警记录	17
4.4.2	告警策略	19
4.4.3	告警接收人	20
4.5	审计日志	20
4.5.1	客户日志	21

1 前言

本用户手册主要介绍了快页网站安全监测管理系统的系统架构、使用和管理。通过阅读本文档，用户可以了解系统的基本组成，并使用系统。

本章内容主要包括：

- 文档目的
- 读者对象
- 文档基本内容
- 约定
- 相关文档
- 技术服务体系

1.1 文档目的

通过阅读本文档，使用户能够正确地配置使用系统，实现对网站的安全检测管理，同时能实时监控日志并生成报告，满足合规要求和业务需求。

1.2 读者对象

本用户手册适用于具有基本网络知识的用户和网络管理员阅读。

1.3 文档基本内容

本用户手册包含以下章节：

- 第一章“前言”，介绍了本手册目的、读者对象、各章节的基本内容、文档约定和技术支持信息。
- 第二章“系统简介”，介绍了系统的功能点、组成等。
- 第三章“初次使用系统”，介绍了系统登录和角色权限。
- 第四章“安全管理员”，介绍了安全管理员权限内的所有功能。
- 第五章“用户”，介绍了用户权限内的所有功能。

- 第六章“审计管理员”，介绍了审计管理员权限内的所有功能。

1.4 约定

本文档遵循以下约定：

图形界面操作的描述采用以下约定：

“”表示按钮。

点击（选择）一个菜单项采用如下约定：

点击（选择）**高级管理 > 特殊对象 > 用户**；

文档中出现的提示、警告、说明、示例等，是关于用户在使用本手册过程中需要特别注意的部分，请用户在明确可能的操作结果后，再进行相关配置。

1.5 相关文档

《快页网站安全监测管理系统安装手册》

1.6 技术服务体系

快页公司对于自身所有安全产品提供远程产品咨询服务，广大用户和合作伙伴可以通过多种方式获取在线文档、疑难解答等全方位的技术支持。

2 系统简介

快页网站安全监测管理系统(云网安)对网站基本信息进行扫描评估,如网站使用的 WEB 发布系统版本,使用的 BBS、CMS 版本;检测网站是否备案等备案信息;另外判断目标网站使用的应用系统是否存在已公开的安全漏洞,是否有调试信息泄露等安全隐患等。

本章主要介绍快页网站安全监测管理系统的组成和功能。

2.1 系统组成

快页网站安全监测管理系统主要由 4 个子系统组成。



1. 资产探测子系统

资产探测子系统是整个系统的基础，负责收集各种资产，查看网页是否含有未登记资产，方便用户能够更加清楚的查看到自己所有的资产信息。

2.内容检测子系统

内容检测子系统支持对网站的内容进行检测，查看系统是否被挂马、包含暗链、敏感文字。

3.漏洞扫描子系统

漏洞扫描子系统支持执行多网站的漏洞扫描，并显示网站是否含有高危漏洞等漏洞信息。

4. 应用监控子系统

应用监控子系统支持对网站应用的安全检测，防止系统应用出现病毒，对网站端口和协议进行扫描，检测是否在正常运行。

2.2 系统功能

2.2.1 资产探测

通过添加网站的 URL，快页网站安全监测管理系统能够扫描添加网站的 URL，扫描出该 URL 下所有网站地址。

2.2.2 内容检测

快页网站安全监测管理系统检测网站内容含有多少 URL 链接，暗链以及敏感文字。

➤ 条件查询

支持多条件组合查询网站，查询结果可以导出查看。如果不输入条件，默认查询所有该时间段内日志。查询结果倒序显示，也就是最新添加的网站在前面。

➤ 报表导出

快页网站安全监测管理系统存储资产信息，以便能够最大限度还原原始信息，为准确取证提供保障。

2.2.3 漏洞扫描

快页网站安全监测管理系统检查各种主机和应用系统漏洞的专业扫描系统，是目前唯一支持 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。

2.2.4 应用监控

快页网站安全监测管理系统检查主机所开放的端口信息、设备状态、响应时间等，可监控应用系统的状态。

2.2.5 告警管理

快页网站安全监测管理系统能够对系统状态和关键事件及时作出响应。目前支持邮件、短信、页面展示等多种响应方式。

3 初次使用系统

本章面向初次接触使用快页网站安全监测管理系统的用户，介绍如何登录系统以及管理系统的三种角色权限。本章内容主要包括：

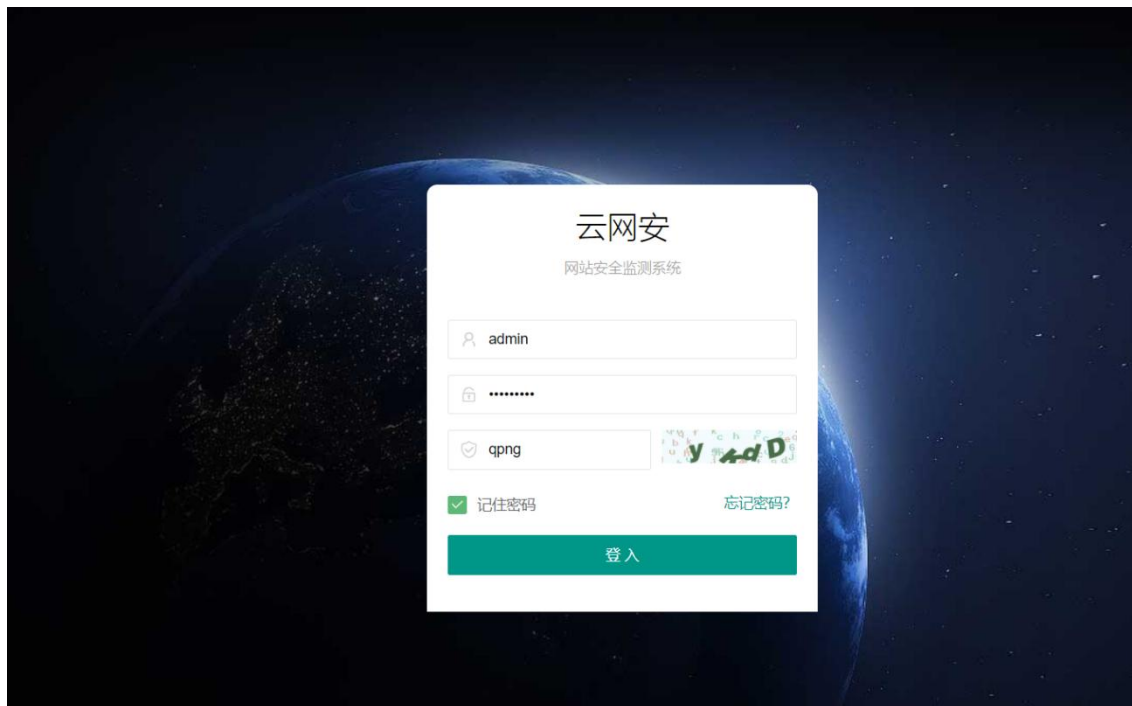
- 系统登录，介绍如何通过默认帐户登录系统。
- 角色权限，介绍管理系统的三种角色权限。

3.1 系统登录

用户在登录系统前应首先在网络中部署和安装快页网站安全监测管理系统服务器，安装并启动成功后，才能正常登录和管理系统。快页网站安全监测管理系统的安装请参见《快页网站安全监测管理系统安装手册》。

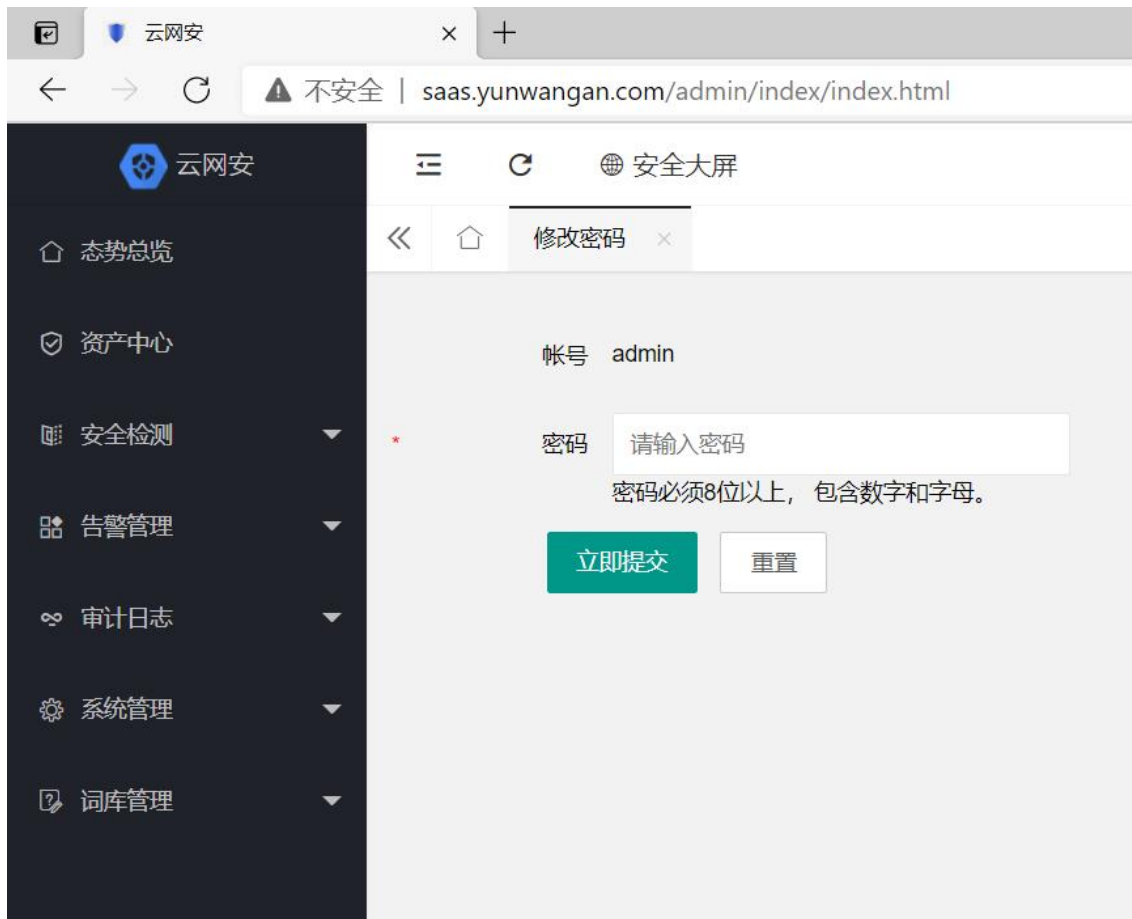
登录系统的具体方法为：

1) 管理员可以通过 HTTP 协议以 WEB 访问的方式对快页网站安全监测管理系统进行远程管理。在访问时，管理员需要在管理主机的浏览器地址栏中输入系统服务器的管理 URL，例如：<http://saas.yunwangan.com/>，进入如下的登录页面。



对应系统的三类管理员角色，系统预置了三个管理员包括：审计管理员 `secauditor`、用户 `sysadmin` 和安全管理员 `secadmin`（默认密码均为 123456），初次登录系统时可使用这三个账号进行相应权限的操作。

2) 点击登录页面的“更改密码”链接，可以修改管理员的登录密码。



输入新密码后，点击“提交更改”按钮，便可完成密码的修改。修改密码后，系统会自动跳转至登录页面，此时需要管理员利用新密码重新登录系统。

3.2 角色权限

快页网站安全监测管理系统依据三权分立的设计原则将用户角色分为以下三个类别，不同的角色对系统拥有不同的管理权限：

- 安全管理员：权限包括主页、用户管理。
- 用户：权限包括主页、日志管理、风险管理、告警管理、报表管理和系统 设置。
- 审计管理员：权限包括主页、系统自审计日志管理。

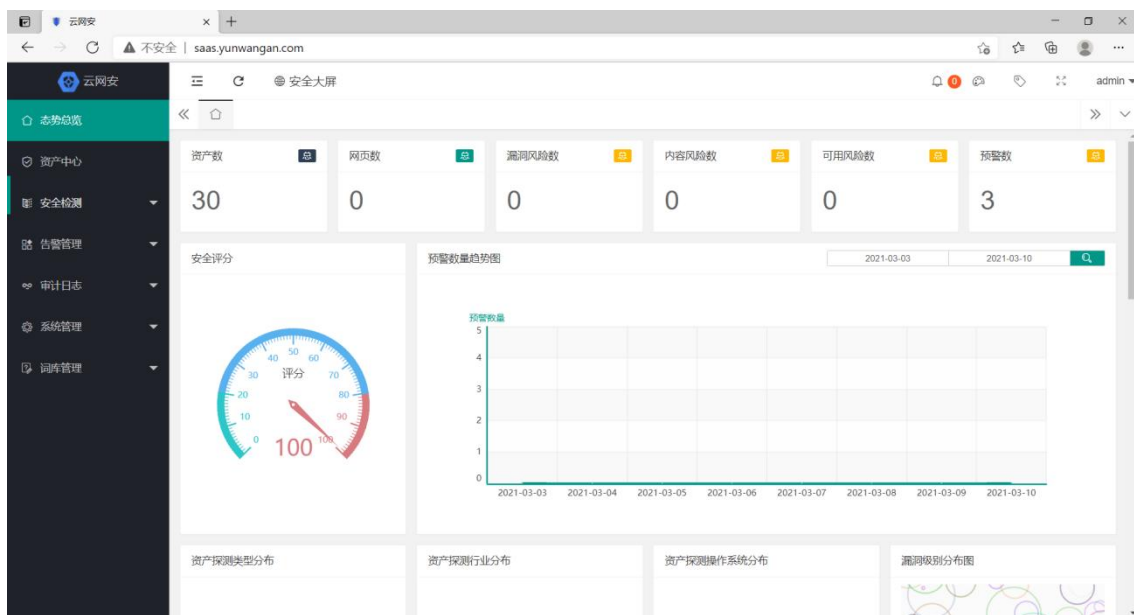
管理员以不同角色登录即拥有不同的管理权限，本手册将依据以上三种角色权限对系统功能进行详细介绍。

4 普通用户

普通用户由平台管理员开设账号，拥有监视主页、安全监测和告警管理的浏览权限。

4.1 主页

用户登录系统后即进入系统主页，如下图所示。

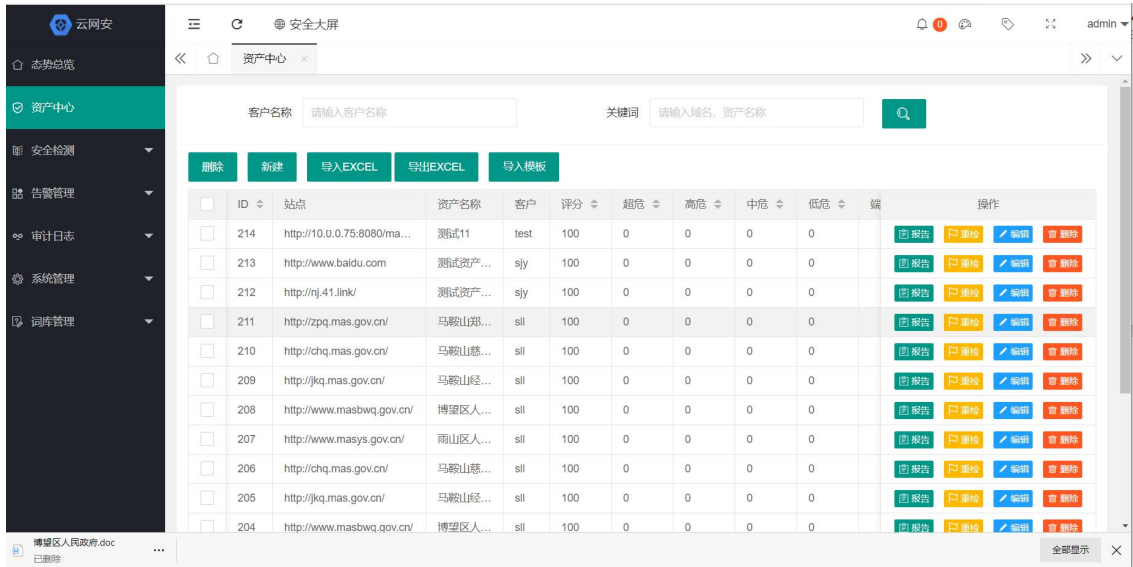


菜单栏：根据角色不同，显示不同的菜单项。

主页中显示了安全评分、预计数量趋势图、漏洞风险数、内容风险数、可用风险数、告警数、资产数，网页数、资产探测类型分布、资产探测行业分布、资产探测操作系统分布、漏洞级别分布图等信息。

4.2 资产中心

通过配置网页信息，快页网站安全监测管理系统能够收集网站信息，并可对系统安全性进行评分，显示系统问题级别。同时，系统为用户提供资产信息导出，导入功能。



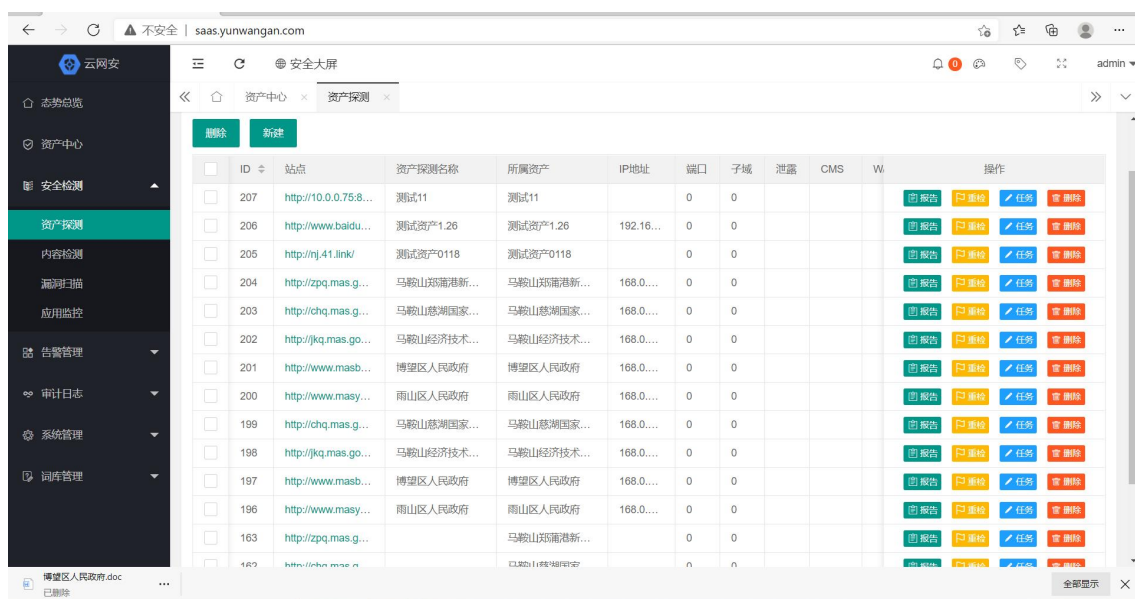
4.3 安全检测

4.3.1 资产探测

实时风险列表提供给管理员实时更新的最近网站风险信息，通过重检功能，管理员可以对网站进行监视、刷新等基本监视条件管理。可以帮助管理员按照不同的网站进行风险监视，进而正确掌握网站的风险情况。

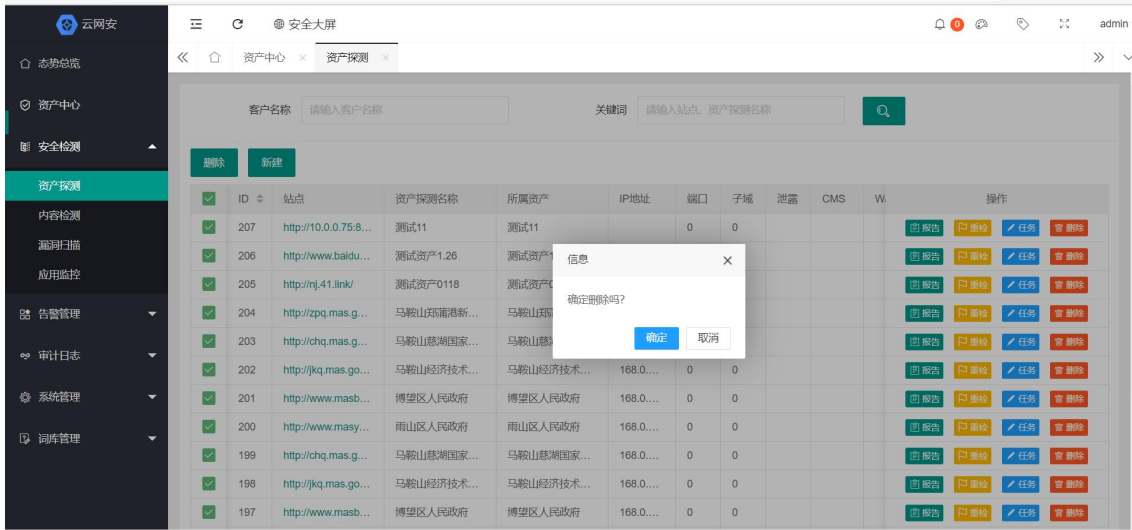
1) 实时风险查看

选择安全检测>资产探测，右侧页面将显示实时收到的该网站的风险信息，如下图所示。



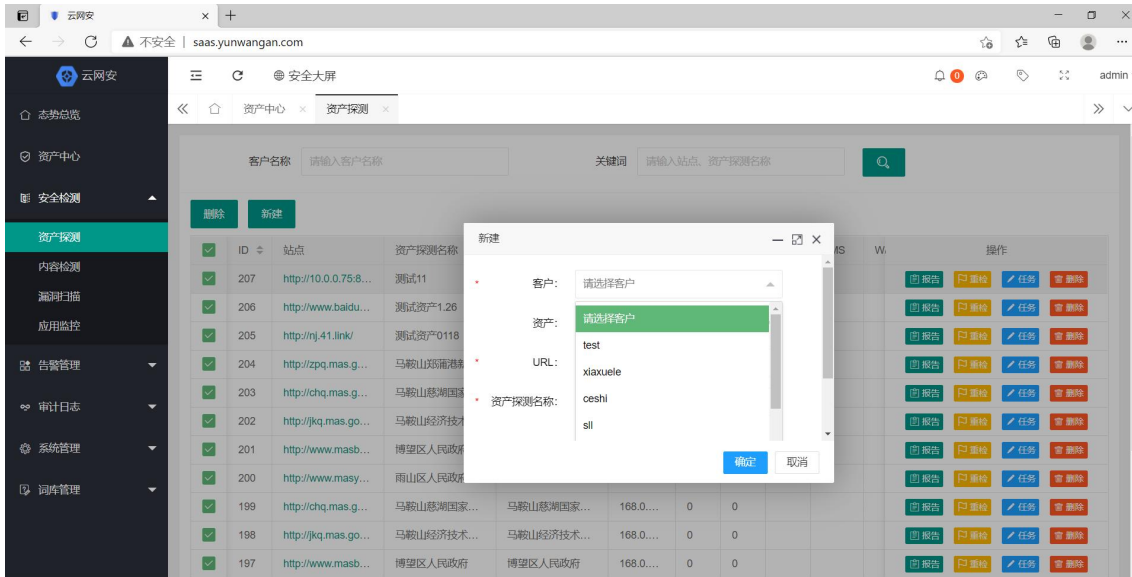
2) 资产删除

点击资产列表上方的“删除”按钮可以清空页面内的站点信息。



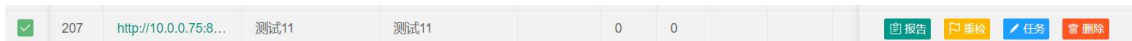
3) 资产添加

点击风险列表上方的“添加”按钮可以添加新的站点信息，填写站点信息，系统会对站点进行扫描。



4) 报告导出

可以选择右侧的“报告”进行资产信息导出。



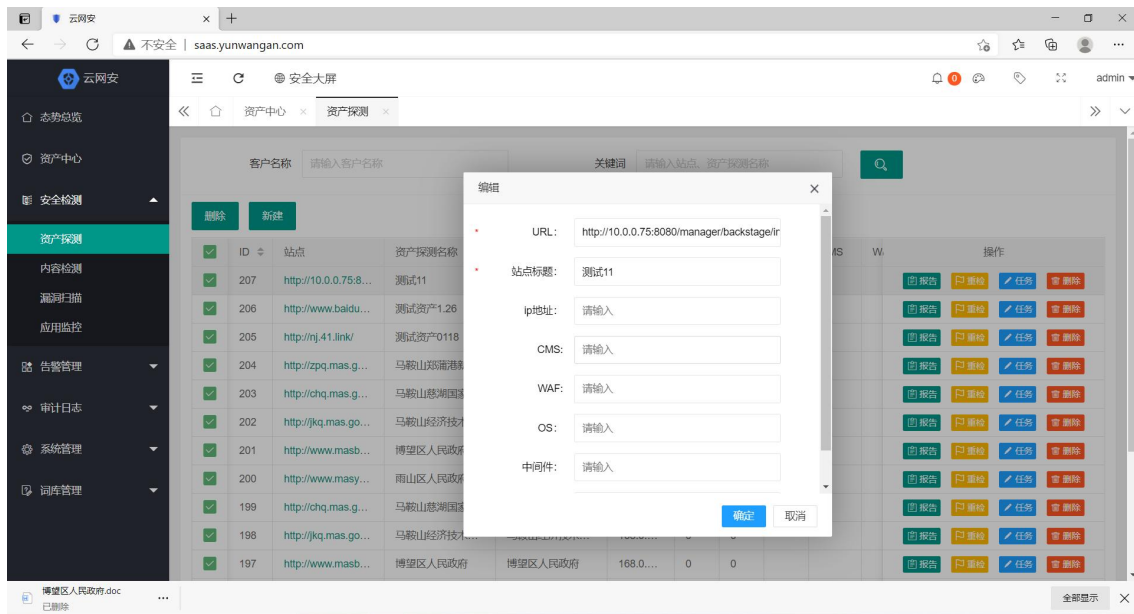
5) 资产查询

管理员可以通过客户名称和关键词对资产进行查询。



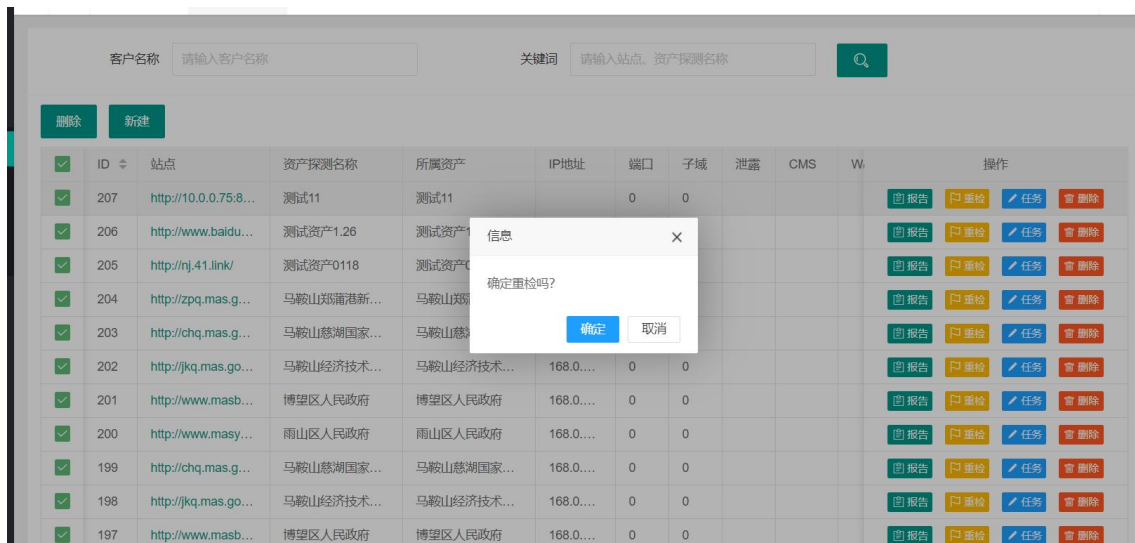
6) 任务发布

用户在右侧任务列表中下发任务，系统对网站进行检测



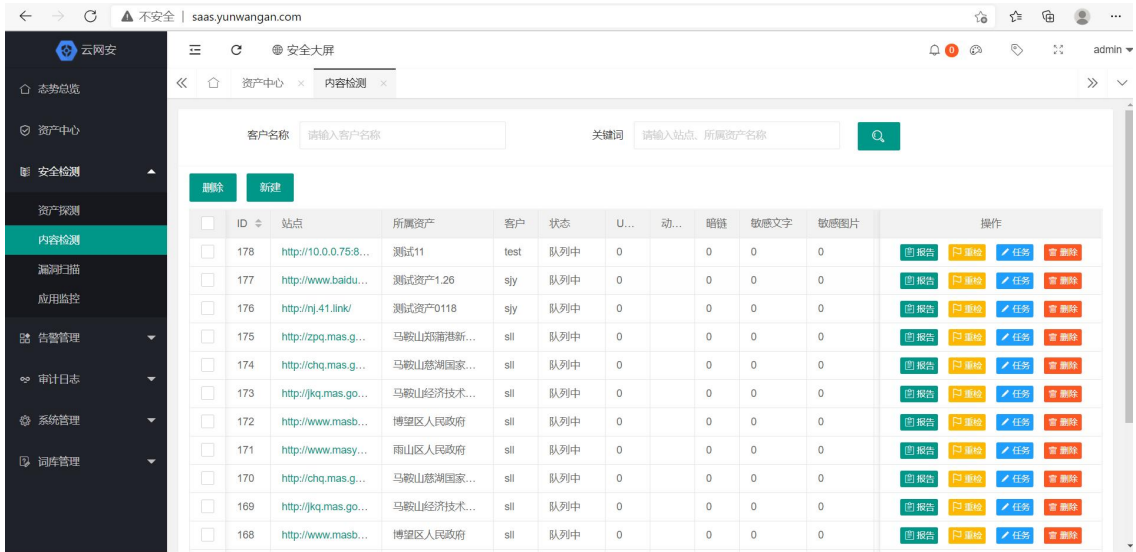
7) 网站重检

点击右侧“重检”，系统重新对网站进行检测，获得最新数据



4.3.2 内容检测

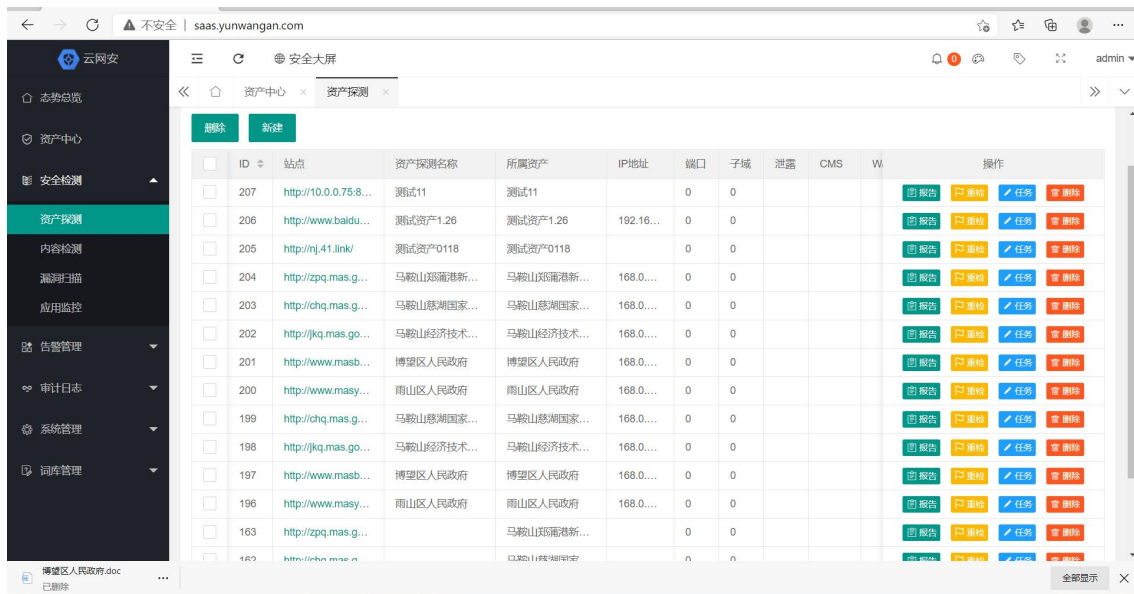
内容检测主要显示网站的 URL，是否被挂马，是否含有暗链，并以表格形式在网页中显示。如下图所示：



此模块提供查询功能，用户通过下拉列表选择年份与月份、日期、日志源，点击“查询”按钮，即可显示出统计结果。

1) 实时风险查看

选择安全检测>内容检测，右侧页面将显示实时收到的该网站内容的风险信息，如下图所示。



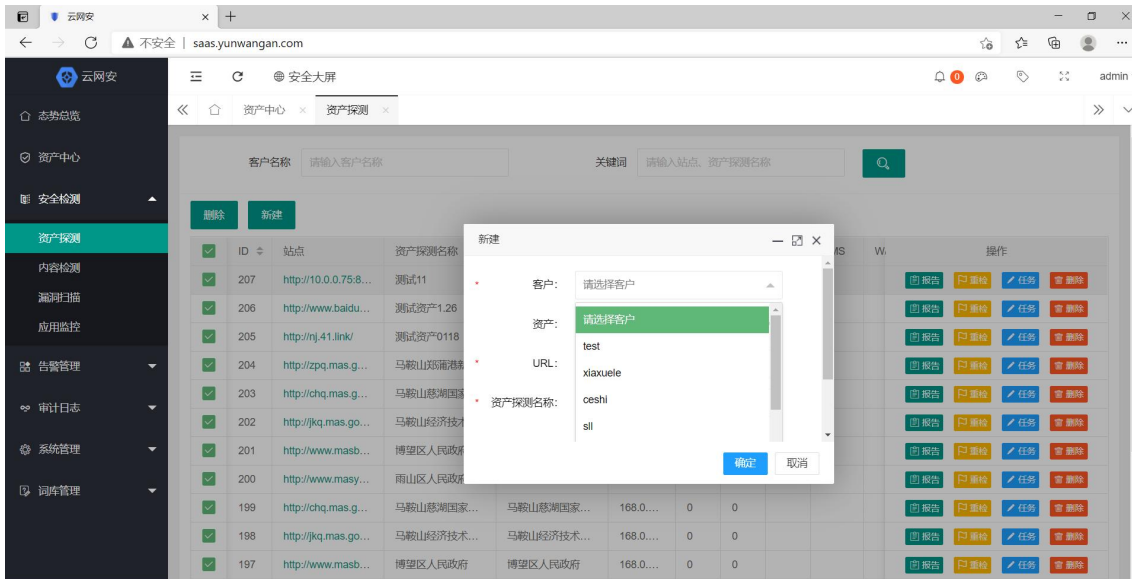
2) 资产查询

管理员可以通过客户名称和关键词对资产进行查询。



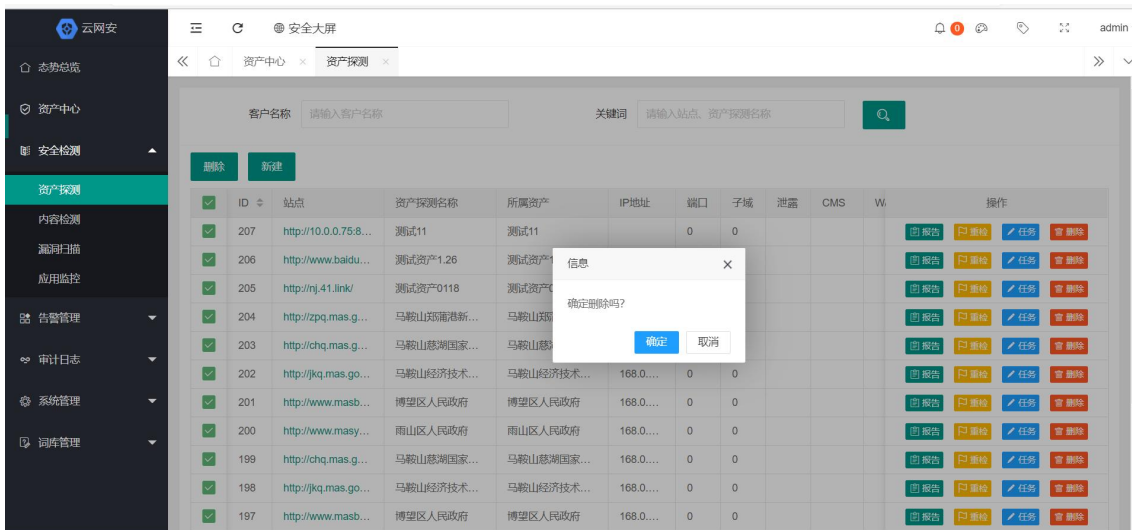
3) 资产添加

点击风险列表上方的“添加”按钮可以添加新的站点信息，填写站点信息，系统会对站点进行扫描。



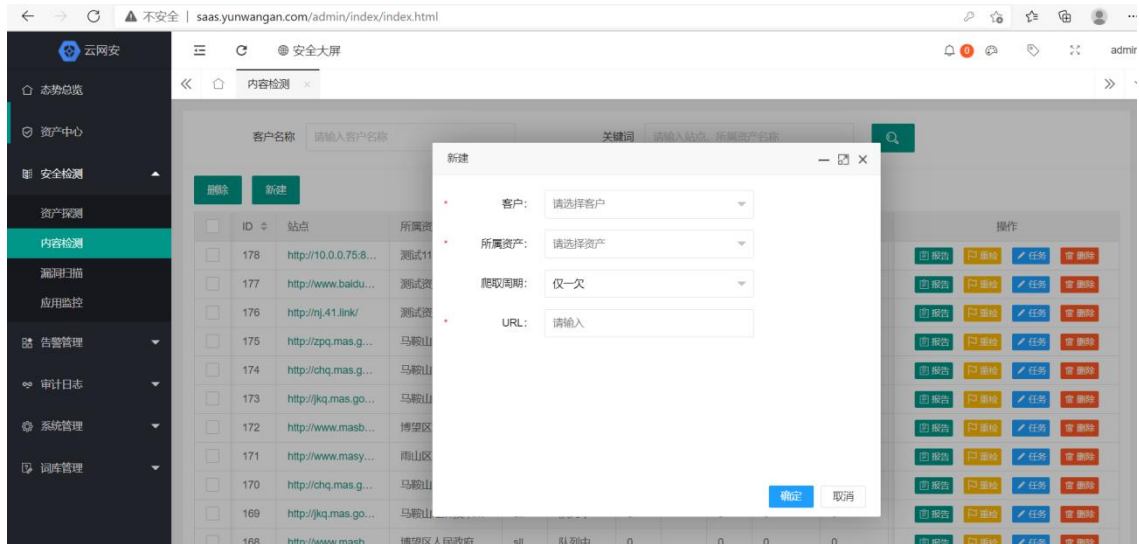
4) 资产删除

点击资产列表上方的“删除”按钮可以清空页面内的站点信息。



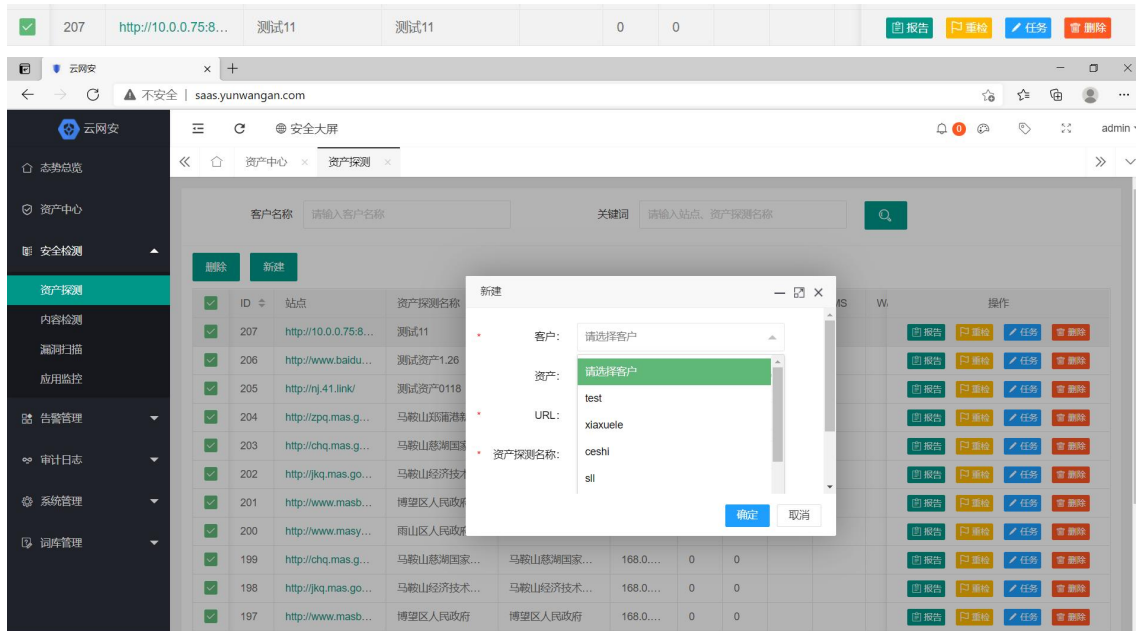
5) 资产添加

点击风险列表上方的“添加”按钮可以添加新的站点信息，填写站点信息，系统会对站点进行内容扫描。



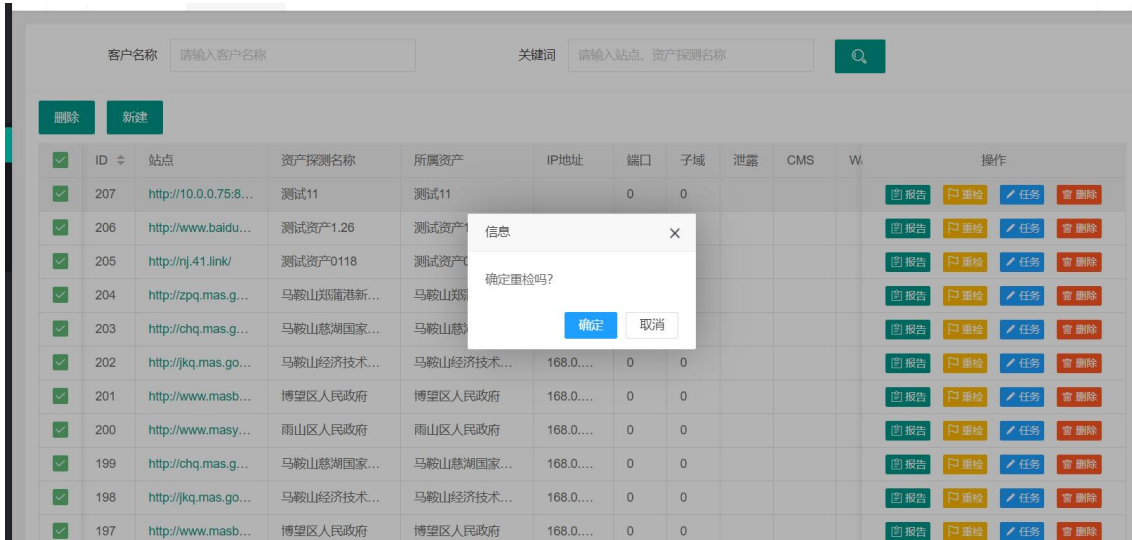
6) 报告导出

可以选择右侧的“报告”进行资产信息导出。



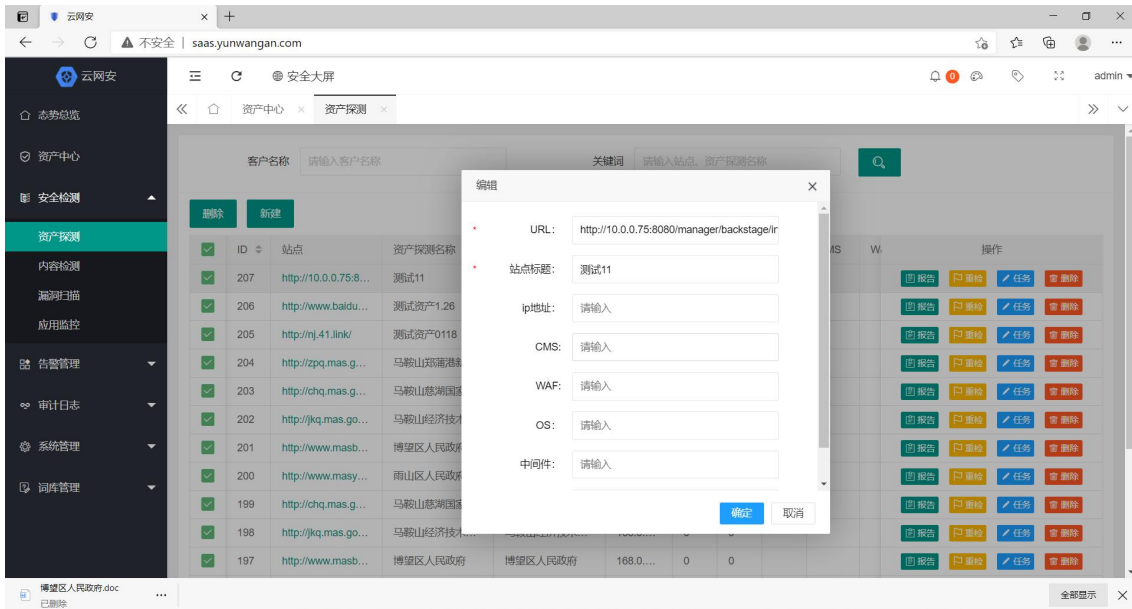
7) 网站重检

点击右侧“重检”，系统重新对网站内容进行检测，获得最新数据



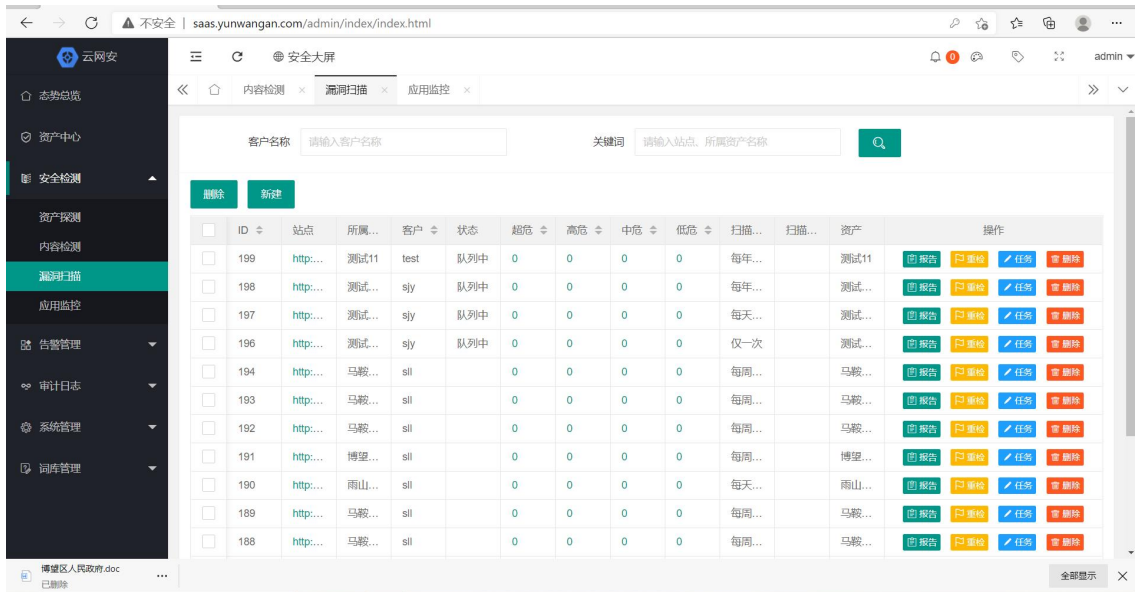
8) 任务发布

用户在右侧任务列表中下发任务，系统对网站内容进行检测



4.3.3 漏洞扫描

漏洞扫描功能是检查各种主机和应用系统漏洞的专业扫描系统，是目前唯一支持 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。



4.3.4 应用监控

应用检测通过协议和端口号对系统应用进行检测，显示应用状态是否正常运行

4.4 告警管理

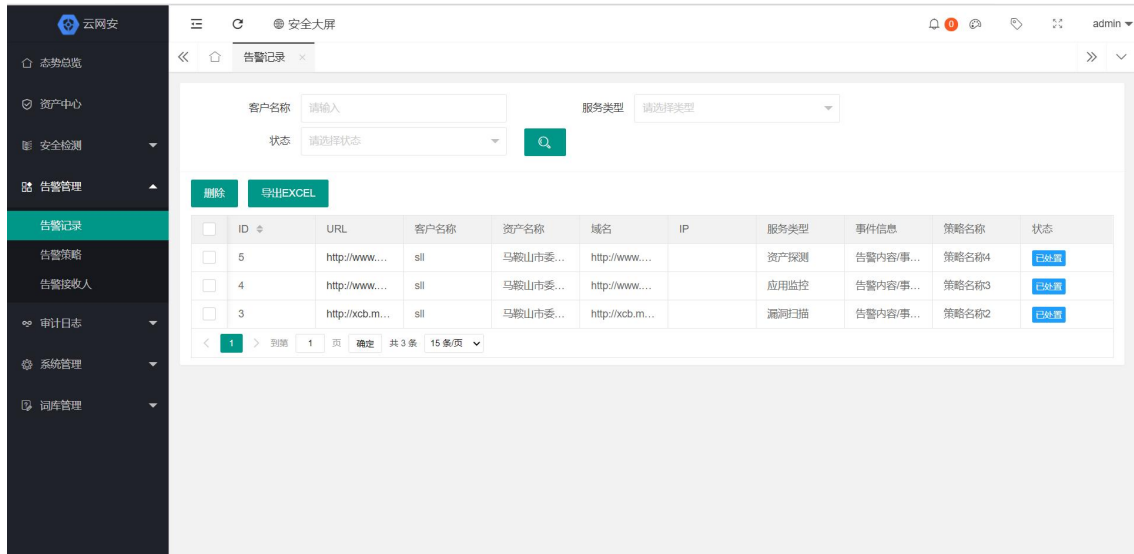
快页网站安全监测管理系统能够对系统状态和关键事件等进行监控，制定不同的规则，及时发现并实时产生告警，便于用户随时了解系统运行情况。

4.4.1 告警记录

实时告警列表提供给管理员实时更新的最近告警信息，通过实时告警功能，管理员可以对告警进行监视、刷新、清零等基本监视条件管理。可以帮助管理员按照不同的告警源进行告警监视，进而正确掌握系统的告警情况。

1) 实时告警查看。

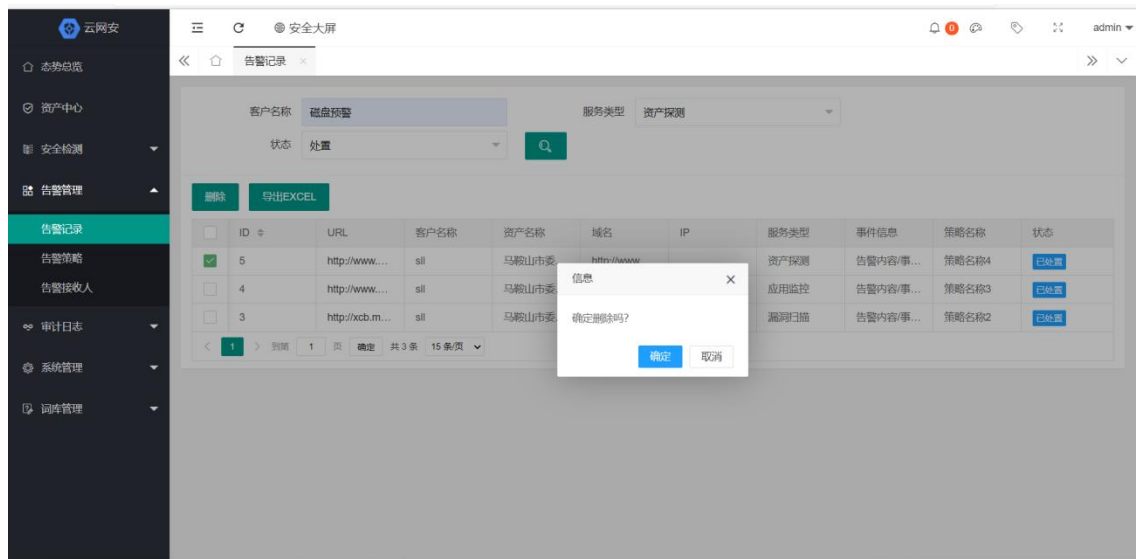
选择告警管理>告警记录，右侧页面将显示实时收到的该网站的告警信息，如下图所示。



点击“某条告警”可以查看告警详情信息。

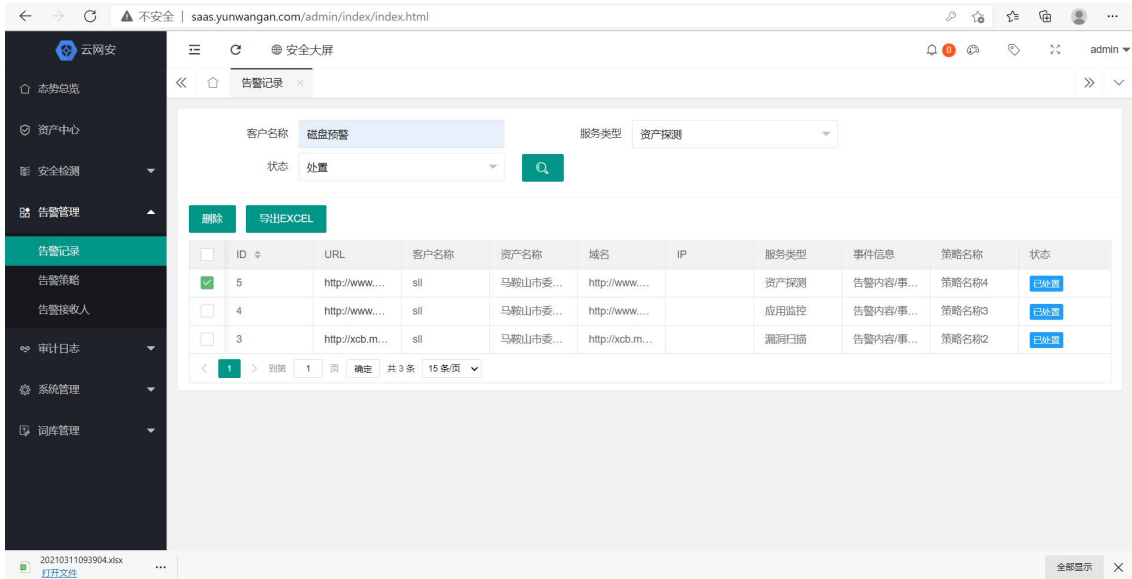
2) 告警清理。

点击告警列表上方的“清理”按钮可以清空某个时间点之前的告警信息。



3) 告警导出。

点击告警列表上方的“导出 EXCEL”按钮可以导出当前页的告警列表，支持导出 EXCEL 文件。



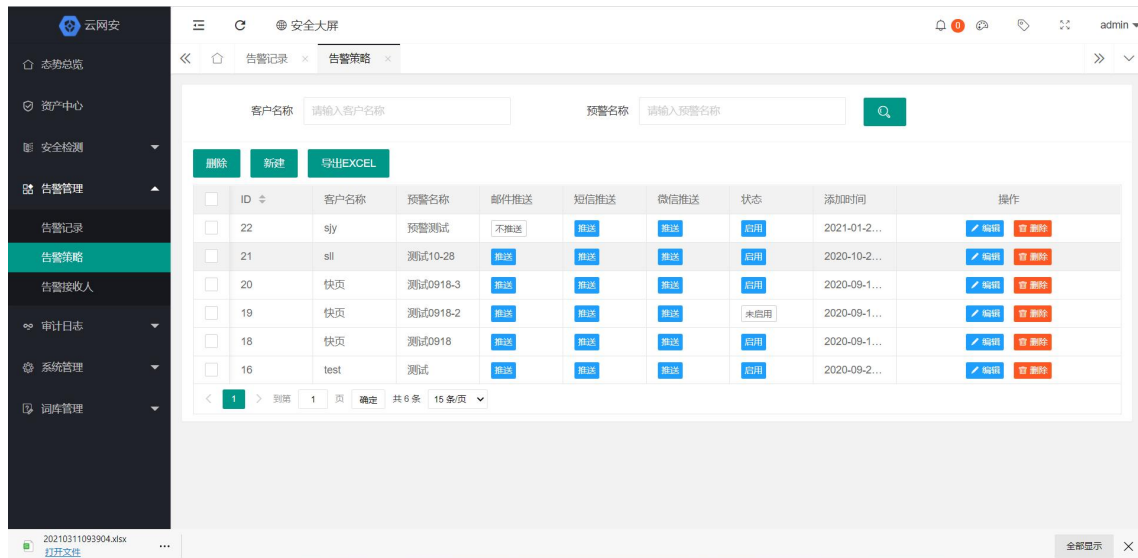
4) 告警查询。

可以选择上方的查询条件进行组合查询。



4.4.2 告警策略

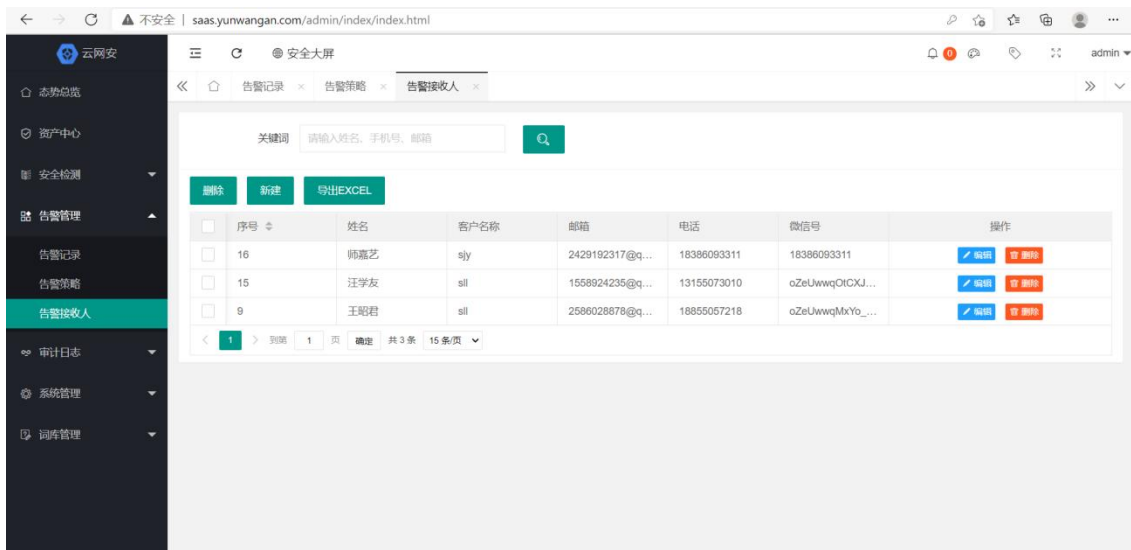
告警设置主要用于告警规则的设置，从而将具有风险的时间进行信息推送。如果告警规则已经与某种类型的响应方式进行了关联，那么系统在产生该告警的同时也会触发响应，响应方式包括页面列表显示、短信通知、邮件通知。



此模块提供查询功能，用户通过“客户名称”、“预警名称”，点击“查询”按钮，即可显示出告警策略。

4.4.3 告警接收人

告警接收人主要用于告警接收人的设置，从而将具有风险的时间进行信息推送。如果告警规则已经与某种类型的响应方式进行了关联，那么系统在产生该告警的同时也会发送给接收人，发生方式包括短信通知、邮件通知。



r

点击“新建”按钮，可以添加一位告警接收人。

4.5 审计日志

云网安系统可以对收集的系统日志进行详尽的分析及统计，同时它具有丰富的报表功能，可以将报表结果分类显示。系统提供了 EXCEL 报表模板。

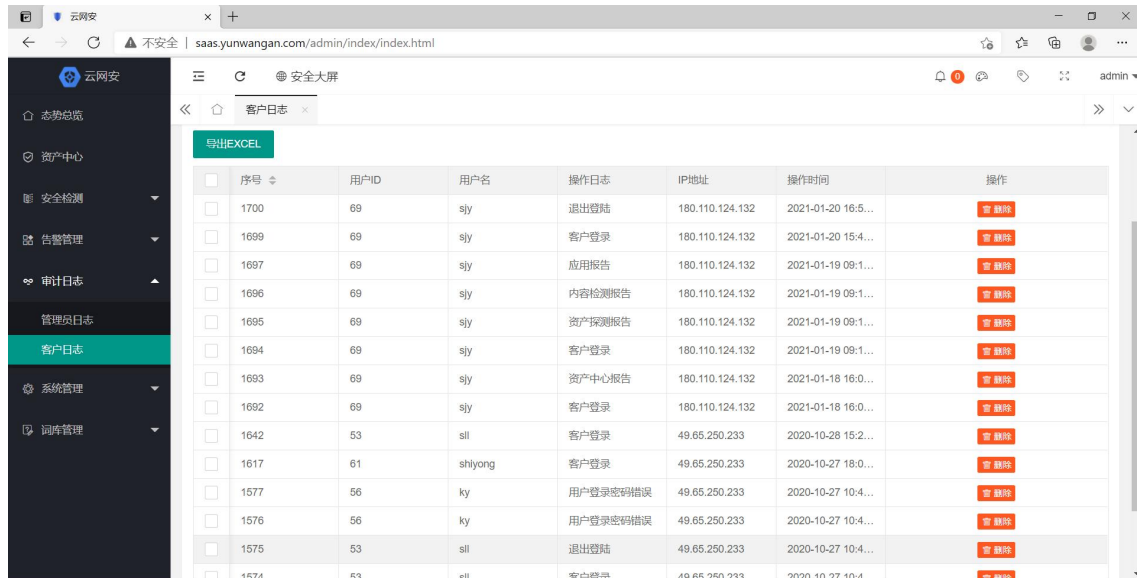
日志功能主要分为管理员日志和客户日志。

4.5.1 客户日志

快页网站安全监测管理系统可以设定在每年、每月、每周或每天的某个时间，自动生成报告。

新建计划报告的操作如下：

1) 选择**报告管理>报告设置**，进入计划报告管理页面，如下图所示。



序号	用户ID	用户名	操作日志	IP地址	操作时间	操作
1700	69	sjy	退出登陆	180.110.124.132	2021-01-20 16:5...	删除
1699	69	sjy	客户登录	180.110.124.132	2021-01-20 15:4...	删除
1697	69	sjy	应用报告	180.110.124.132	2021-01-19 09:1...	删除
1696	69	sjy	内容检测报告	180.110.124.132	2021-01-19 09:1...	删除
1695	69	sjy	资产探测报告	180.110.124.132	2021-01-19 09:1...	删除
1694	69	sjy	客户登录	180.110.124.132	2021-01-19 09:1...	删除
1693	69	sjy	资产中心报告	180.110.124.132	2021-01-18 16:0...	删除
1692	69	sjy	客户登录	180.110.124.132	2021-01-18 16:0...	删除
1642	53	sll	客户登录	49.65.250.233	2020-10-28 15:2...	删除
1617	61	shiyong	客户登录	49.65.250.233	2020-10-27 18:0...	删除
1577	56	ky	用户登录密码错误	49.65.250.233	2020-10-27 10:4...	删除
1576	56	ky	用户登录密码错误	49.65.250.233	2020-10-27 10:4...	删除
1575	53	sll	退出登陆	49.65.250.233	2020-10-27 10:4...	删除
1574	53	sll	客户登录	49.65.250.233	2020-10-27 10:4...	删除

2) 系统已内置自动报告，可开启或关闭，如开启，系统将自动在某时间点生成日报、周报、月报、年报。

3) 点击“新建”添加定制报告，弹出如下窗口。



在弹出的窗口中输入计划报告名称，在“时间范围”右侧日期的下拉菜单中选择时间区间。如果选择的结束时间是未来时间，则系统在结束时间到达时生成报告；如果选择的结束时间是历史时间，则系统立即生成报告。