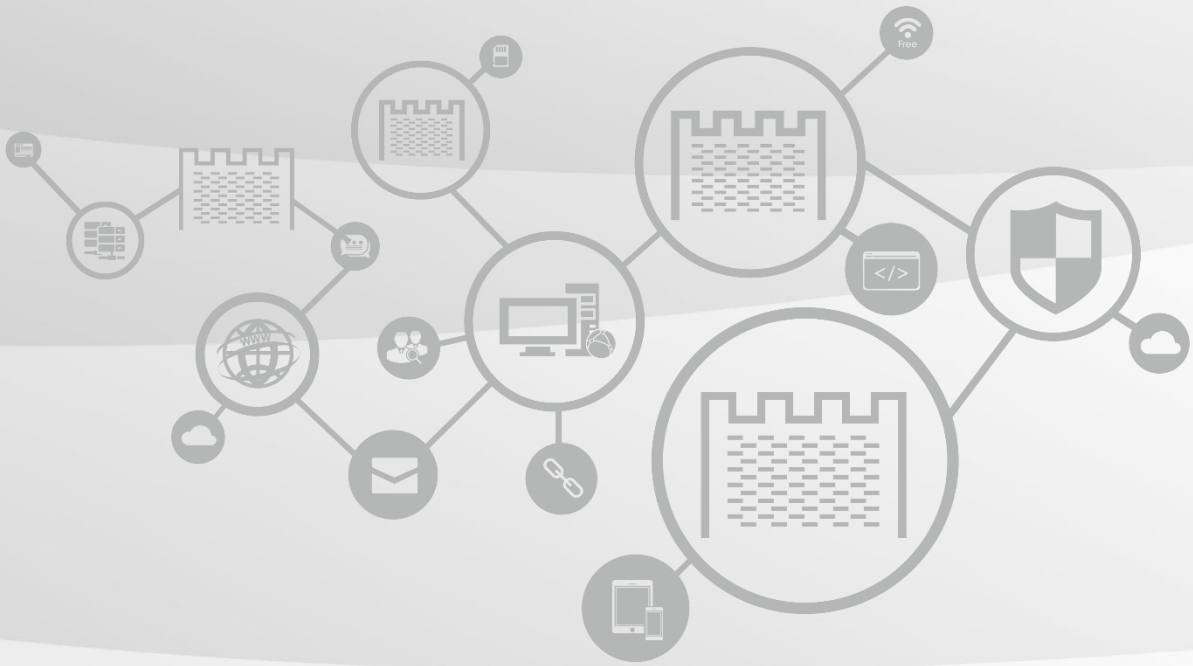
网站监控预警平台 V3.0 用户手册



远江盛邦（北京）网络安全科技股份有限公司

http：//www.webray.com.cn

[部门名称]

■ 文档编号		■ 密级	
■ 版本编号		■ 日期	20190830
■ 撰 写 人	李晶晶	■ 批准人	

■ 版本变更记录

时间	版本	说明	修改人
20190830	V3.0(3.0.4-R1-47934-20190815143215)	新增	李晶晶
20210409		修改	梁艳

目录

1.产品概述

1.1 产品简介

网站监控预警平台是远江盛邦公司专门针对网站频发的安全事件精心研发的一款监控预警产品。该产品主要从四个方面进行全方位不间断监控。主要以各种技术手段对网站的可用性、完整性、安全性进行安全监控。它的设计思路是帮助客户主动发现问题、及时处理和响应问题、并便于对大规模网站监控、从而减低客户人工成本等方面。

网站监控预警平台能够主动监控网站安全问题，监测网站脆弱性。并提供专业的修补意见，降低安全风险，防范于未然。并且提供网站监控平台 7*24 小时不间断监控，保持监控的持续性。突发攻击事件发生时，及时进项响应与处理，构建完善的网站安全体系。对于大范围的网站利用自动化的技术手段进行监控，减低人工成本。通过统一的指标进行全方位监控，为统一监管提供技术依据和关键指标。

2.基础配置向导

2.1 操作管理员部分

2.1.1 监视概要

监视概要功能就是统一显示云监控区域的概略结构，监控概要界面可以查看节点信息、系统资源使用率、风险总览、网站风险排行和安全问题汇总等信息。在主页面中选择“监控概要”，进入监控概要界面。

2.1.1.1 目标系统监控区域

可以查看全国威胁区域（攻击源地点动态展示）

1. 支持选中地图上安全事件显示地方安全事件并在告警颜色条上同步告警等级程度，点击跳转到网站详情查询。（现点击无事件的地图仍支持跳转）。
2. 刷新界面，保存不同规格的地图（地图可放缩保存）；选中地图上安全事件按区域默认保存图片格式为 png，大小 650X337。

图 2.1-1 实时分析图

2.1.1.2 网络空间攻防动态

网站实时攻防动态展示，用不同颜色区分攻击强度。攻击源的地理位置以及攻击来源（WAF、DDOS），能记录近 500 条攻防数据。

图 2.1-2 攻防实时状态展示图

2.1.1.3 每日监控事件

2.1.1.3.1 监控统计

通过两种方式（拆线图切换、柱形图切换）展示监控事件内容，默认展示如下图:

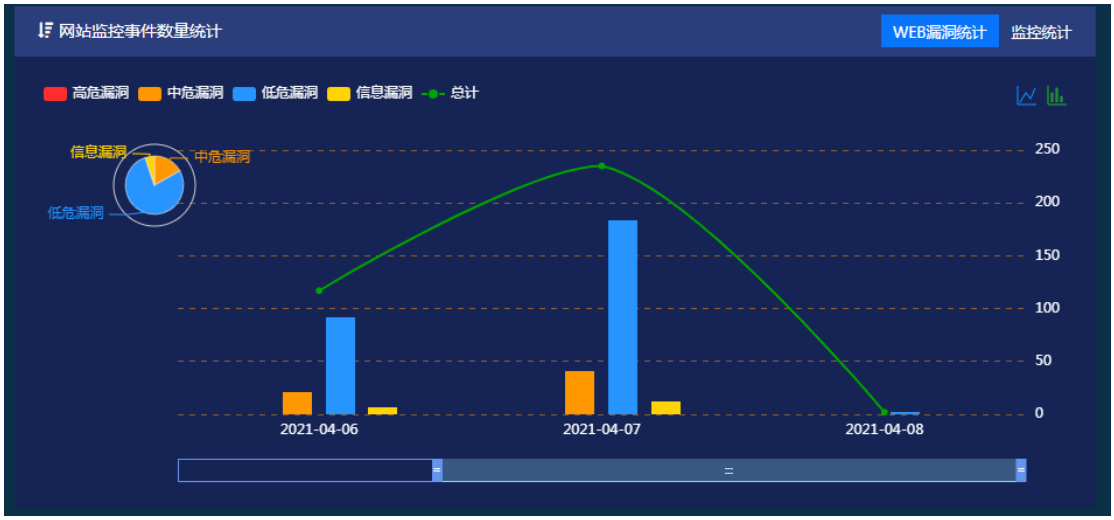


图 2.1-3 每日监控事件

2.1.1.3.2 漏洞统计

通过三种方式（数据视图、拆线图切换、柱形图切换）展示监控事件中存在的漏洞，默认为柱形图展示可自行选择展示方式。

图 2.1-4 漏洞统计

2.1.1.4 监控事件排名

2.1.1.4.1 web 漏洞信息

通过两种方式（拆线图切换、柱形图切换）展示监控事件可用性程度，默认为拆线图展示可自行选择展示方式。

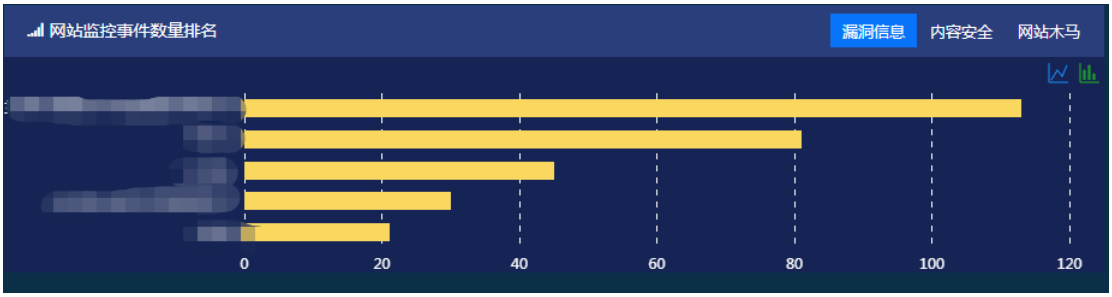


图 2.1-5 可用性

2.1.1.4.2 内容安全

通过两种方式（拆线图切换、柱形图切换）展示监控事件内容安全等级，默认为柱形图展示可自行选择展示方式。

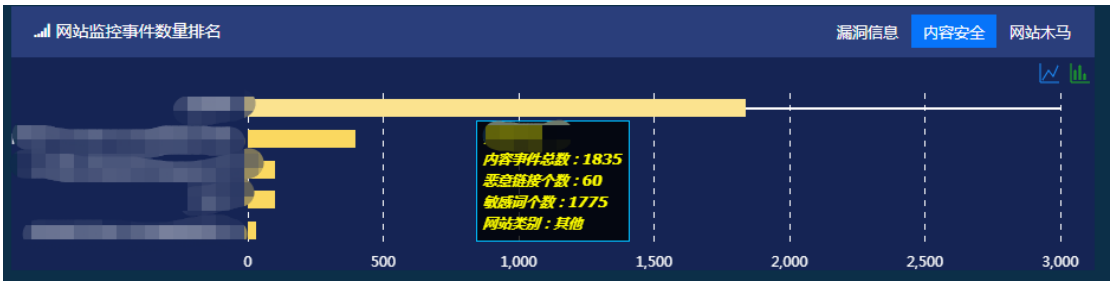


图 2.1-6 内容安全

2.1.1.4.3 木马信息

通过两种方式（拆线图切换、柱形图切换）展示监控事件中漏洞信息量，默认为柱形图展示可自行选择展示方式。

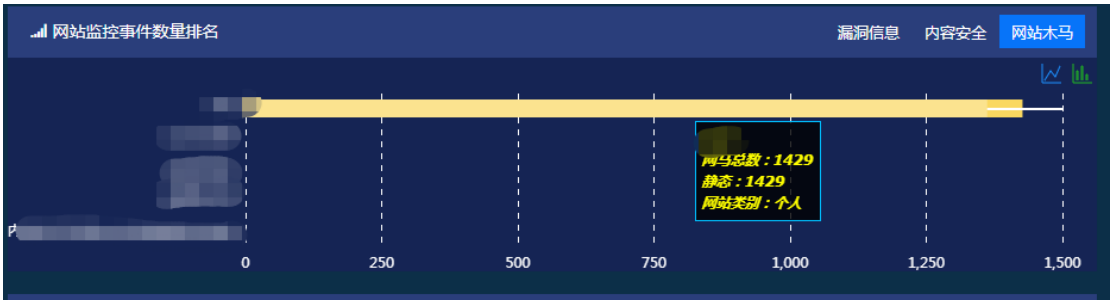


图 2.1-7 木马信息

2.1.1.5 网站概况

2.1.1.5.1 实时事件

监控事件中监测到的问题会实时的进行展示和实时告警，及时处理问题解决安全隐患。

图 2.1-8 实时事件

2.1.1.5.2 网站评分

对监控事件做出评分，以便运维人员及时做出判断，对网站进行安全加固

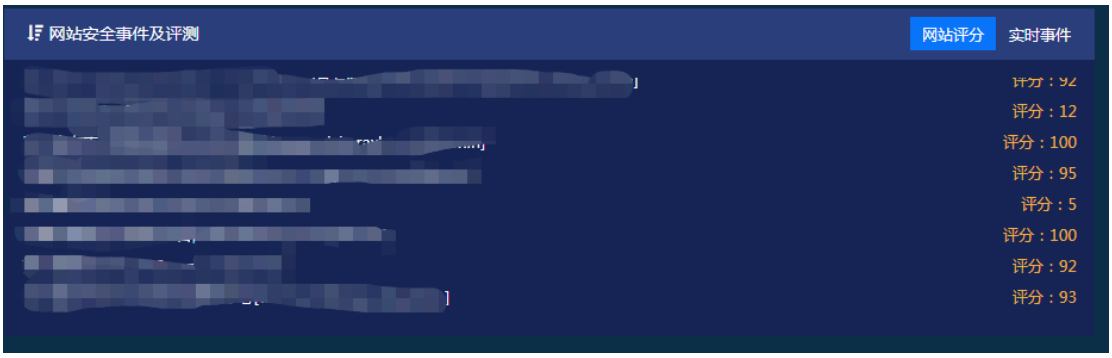


图 2.1-9 网站评分

2.1.2 任务中心

该版本增加一键重启任务功能，在操作管理员账户右上方显示一键重启按钮，选择重启的任务再次执行。一次性可将所以已执行过的任务重启。

2.1.2.1 快速通道

2.1.2.1.1 批量录入

WEBUI：主界面 -> 任务中心 -> 快速通道

通过该功能可以一键式快速配置监控站点，在网站地址处输入域名（例如：http://www.demo.com/），按需求勾选任务项，还可选择可用性任务、内容监控任务的监控周期，使用路线和 web 漏洞的模板选择，点击“录入”按钮完成任务添加，所有任务项为默认开启（不勾选时任务不执行），其余模板均采用默认。如果需要批量添加，点击右侧“下载模版”按钮，下载 SiteTemplet.xls 文件，按照表中格式填写站点信息，保存后点击“浏览”按钮上传，便完成批量站点的导入操作。可支持手动输入 ipv6 格式的目标地址建立任务，批量导入 ipv6 格式的目标地址建立任务，也可通过站点管理添加 ipv6 地址的站点，再通过批量录入-》使用站点列表建立任务。

图 2.1.2-1 手动输入

图 2.1.2-2 批量录入

图 2.1.2-3 批量录入

2.1.2.2 站点管理

2.1.2.2.1 站点管理

WEBUI：主界面 -> 任务中心 -> 站点管理

管理该站点的信息，包含站点名称、监控地址、创建时间、网站类别、地区

以及所属用户。通过界面搜索框按名称/域名/类别/用户名搜索。也可通过高级检索按站点名称、监控地址、创建时间、网站类别、地区、所属用户来查询。

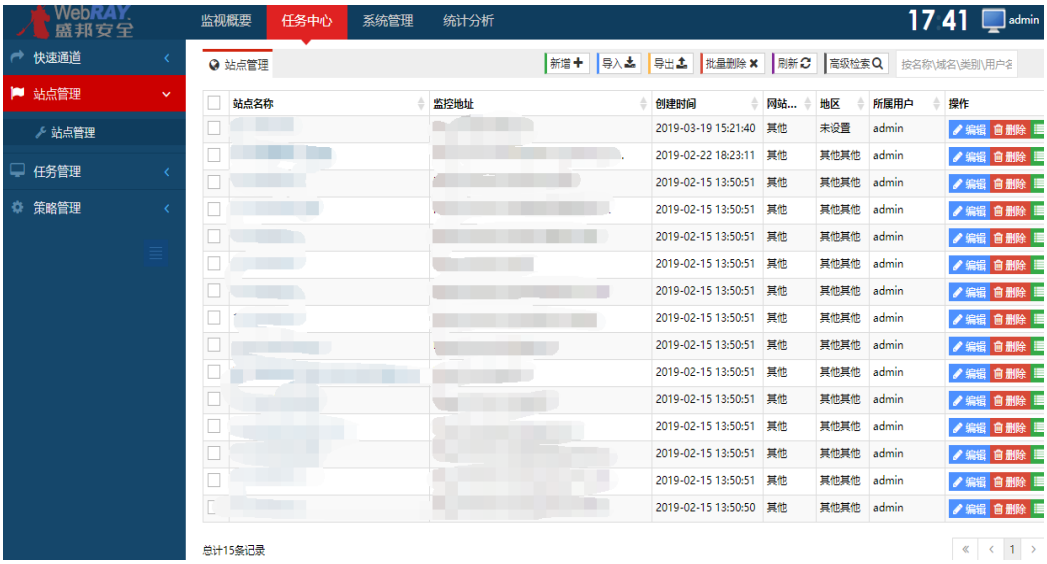


图 2.1.2-4 站点管理

WEBUI：主界面 -> 任务中心 -> 站点管理->站点新增

新增导入对单个站点，和站点编辑一致可对该站点进行基本信息、指纹信息、资产信息、认证配置、代理服务器设置、站点白名单设置、网络连接设置和扫描高级选项设置。此外可根据导入站点信息判断站点所属 ip 和域名。支持添加 ipv6 格式的站点。

图 2.1.2-5 站点新增基本选项

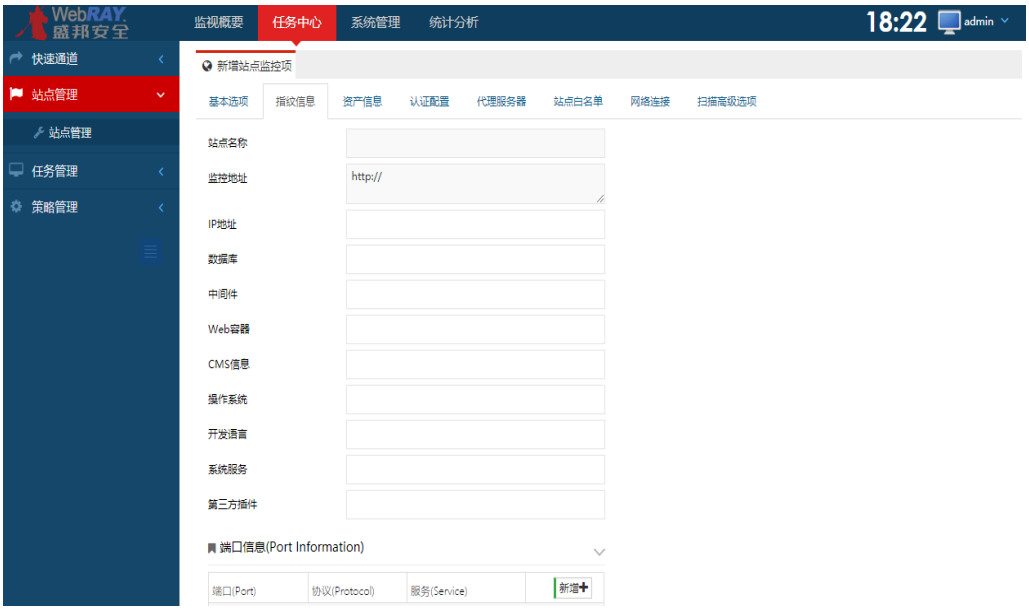


图 2.1.2-6 站点新增/编辑指纹信息

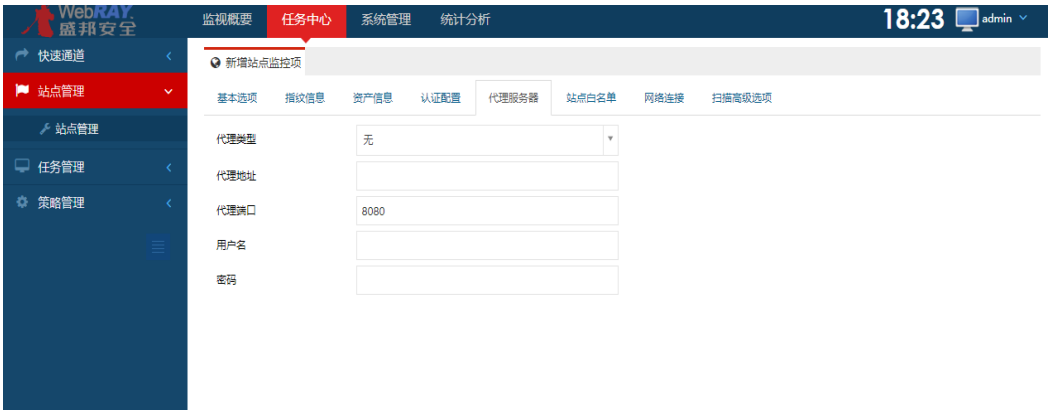


图 2.1.2-7 站点新增/编辑代理配置

图 2.1.2-8 站点新增站点白名单配置

图 2.1.2-9 站点网络链接设置

图 2.1.2-10 站点扫描高级选项设置

WEBUI：主界面 -> 任务中心 -> 站点管理->删除/批量删除

批量删除操作可以对一个/多个站点同时进行删除，须注意删除站点会同时删除站点所相关的任务信息。

WEBUI：主界面 -> 任务中心 -> 站点管理->站点导入

导入操作可以先根据下载模板填写站点，再次导入站点即创建站点信息，可在站点管理界面查询或编辑。注意的是站点管理里只添加站点信息不会同步生成任务信息。

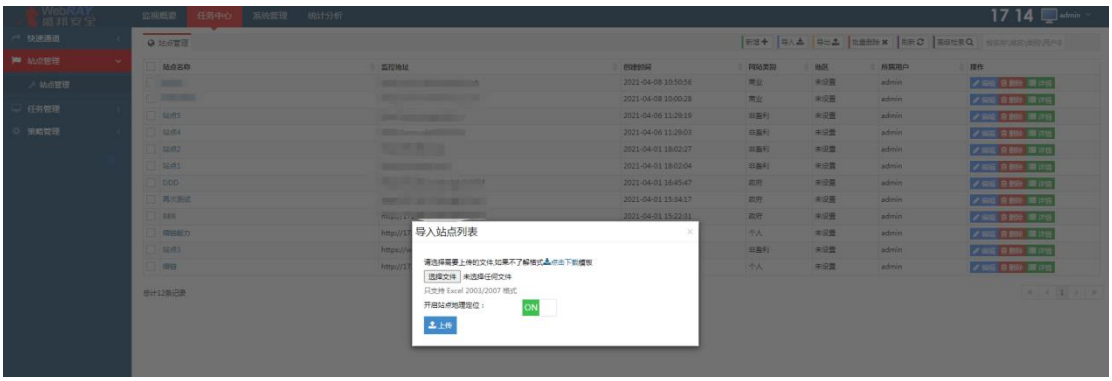


图 2.1.2-11 站点导入

图 2.1.2-12 站点高级检索

WEBUI：主界面 -> 任务中心 -> 站点管理->站点导出

根据所勾选的站点以默认 site_info.xls 进行导出。可勾选全选框将当前页面站点导出，也可勾选多个站点导出。

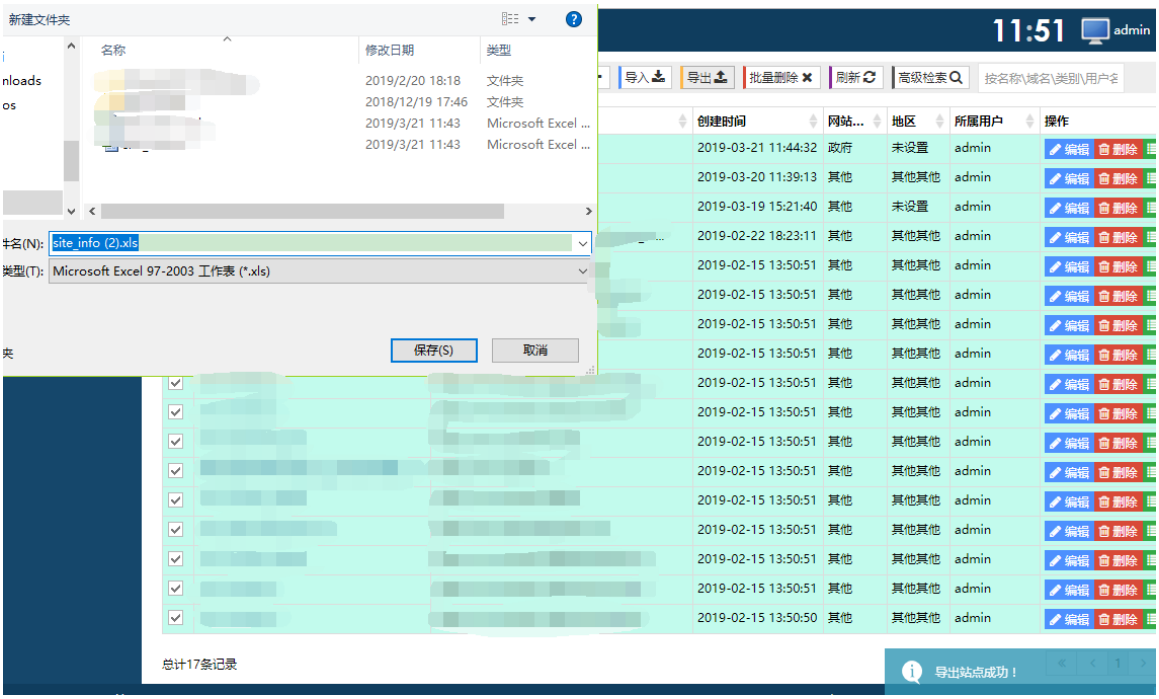


图 2.1.2-13 站点导出

2.1.2.3 策略管理

2.1.2.3.1 网站监控配置

WEBUI：主界面 -> 任务中心 -> 策略管理

针对网站的检测，包含了模板名称、模板类型、监控的描述以及操作。针对

不同任务，可以创建不同的模板。

图 2.1.2-14 网站监控模板配置

2.1.2.3.2 域名检测配置

针对域名的检测的配置，包含了模板名称、模板类型、监控描述以及操作。针对不同的扫描任务，配置不同的检测模板。

图 2.1.2-15 域名检测模板配置

2.1.2.4 任务管理

2.1.2.4.1 HTTP 监控

WEBUI：主界面 -> 任务中心 -> 任务管理 -> HTTP 监控

HTTP 监控：通过 HEAD 请求方式向服务器索要响应，同时对 HTTP 协议端口（默认为 80 端口）进行监控。通过高级检索按照任务名称、站点名称、模

板类型、检测点进行查询。可支持 ipv6 地址的监控。

图 2.1.2-16 HTTP 监控

在主页面选择:任务中心 > 任务管理 > HTTP 监控（admin 等）

1）点击新增>添加任务名称>进行站点选择

2）选择检测点>选择检测周期>选择检测模板>选择报警组模板>选择报警条件

图 2.1.2-17 新增 HTTP 监控任务

监控名称：填写该监控任务的名称。

站点选择：选择进行 http 监控的站点

监测点：可选择默认线路，也可选择自定义的线路。

检测周期：可选择立即执行，每 N 分钟执行一次，每 N 小时执行一次，定时执行，每天执行一次，每周执行一次，每月执行一次。

监控模板：可选择 HTTP 监控模板或自定义模板。

选择报警组：可选择默认报警模板或自定义模板。

报警条件：输入网站响应超时时间，网站响应超时次数。

告警次数：网站触发告警后连续告警次数。

2.1.2.4.2 DNS 监控

WEBUI：主界面 -> 任务中心 -> 任务管理 -> DNS 监控

DNS 监控：监控引擎通过 DNS 服务器对监控域名进行寻址、解析，回报反应速度，监控域名解析的流畅度。通过高级检索按照任务名称、站点名称、模板类型、检测点进行查询。可支持 ipv6 地址的监控。

图 2.1.2-18 DNS 监控

监控名称：填写该监控任务的名称。

站点选择：选择进行 DNS 监控的站点.

监测点：可选择默认线路，也可选择自定义的线路。

检测周期：可选择立即执行，每 N 分钟执行一次，每 N 小时执行一次，定时执行，每天执行一次，每周执行一次，每月执行一次。

监控模板：可选择 DNS 监控模板或自定义模板。

选择报警组：可选择默认报警模板或自定义模板。

报警条件：输入网站响应超时时间，网站响应超时次数。

告警次数：网站触发告警后连续告警次数。

图 2.1.2-19 DNS 新增任务

2.1.2.4.3 PING 监控

WEBUI：主界面 -> 任务中心 -> 任务管理 -> PING 监控

PING 监控：通过 PING 发送一个 ICMP 协议，回声请求消息给目的地并报告是否收到所希望的 ICMP echo，用来检查网络是否通畅和网络连接速度。可支持 ipv6 地址的监控。

图 2.1.2-20 PING 监控

监控名称：填写该监控任务的名称。

站点选择：选择进行 PING 监控的站点

监测点：可选择默认线路，也可选择自定义的线路。

检测周期：可选择立即执行，每 N 分钟执行一次，每 N 小时执行一次，定时执行，每天执行一次，每周执行一次，每月执行一次。

监控模板：可选择 PING 监控模板或自定义模板。

选择报警组：可选择默认报警模板或自定义模板。

报警条件：输入网站响应超时时间，网站响应超时次数。

告警次数：网站触发告警后连续告警次数。

2.1.2.4.4 内容监控

WEBUI：主界面 -> 任务中心 -> 任务管理 -> 内容监控

内容监控：监控网站内容是否被篡改，是否被恶意插入暗链，文字是否含有敏感信息。通过高级检索按照任务名称、站点名称、模板类型进行查询。可支持

ipv6 地址的监控。

图 2.1.2-21 内容监控

监控名称：填写该内容监控任务的名称。

站点选择：选择进行内容监控任务的站点。

监控深度：选择该监控任务的的监控深度。

检测周期：可选择立即执行，每 N 分钟执行一次，每 N 小时执行一次，定时执行，每天执行一次，每周执行一次，每月执行一次。

扫描线程：可设置扫描线程数，最大线程数为 2000，最小线程数为 50。

扫描最大页面数：可选择扫描的最大页面数，最大页面数为 20000，最小为 5。

监控模板：选择默认监控模板（全面检查）或监控模板（精确检查），也可支持自定义模板。

选择报警组：选择默认告警模板。

图 2.1.2-22 新增内容监控任务

2.1.2.4.5 WEB 漏洞扫描

WEBUI：主界面 -> 任务中心 -> 任务管理 -> WEB 漏洞扫描

WEB 漏洞扫描：对一个网站进行漏洞扫描，显示漏洞的数量和名称。通过高级检索按照站点名称、模板名称、任务类型进行查询。可支持 ipv6 地址的扫描。

图 2.1.2-23 WEB 漏洞扫描

监控名称：填写该 web 漏洞扫描任务的名称。

站点选择：选择进行该 web 漏洞扫描任务的站点。

检测周期：可选择立即执行，每 N 分钟执行一次，每 N 小时执行一次，定时执行，每天执行一次，每周执行一次，每月执行一次。

扫描深度：设置该 web 漏洞扫描任务的深度。

扫描线程：可设置扫描的线程数。

扫描最大页面数：可设置该 web 漏洞扫描任务的扫描最大页面数

最大相似连接数：设置该 web 漏洞扫描任务的扫描最大相似连接数。

监控模板：可选择漏洞扫描模板或自定义模板。

选择报警组：选择告警默认模板或自定义告警模板。

图 2.1.2-24 新增 web 漏洞扫描任务

2.1.2.4.6 WebShell 检测

WEBUI：主界面 -> 任务中心 -> 任务管理 -> WebShell 检测

Webshell 检测：webshell 是网站的后门工具，通常会将 asp 或 php 后门

文件与网站服务器 WEB 目录下正常的网页文件混在一起，然后就可以使用浏览器来访问 asp 或者 php 后门，得到一个命令执行环境，以达到控制网站服务器的目的。

图 2.1.2-25 WebShell 检测

2.1.2.4.7 网站木马检查

WEBUI：主界面 -> 任务中心 -> 任务管理 -> 网站木马检查

网页木马检查：网站可能存在的木马病毒使用户的计算机面临风险，所以要检测。通过高级检索按照任务名称、站点名称进行查询。可支持 ipv6 地址的扫描。

图 2.1.2-26 网站木马检查

检测名称：填写该网站木马检查任务的名称。

站点选择：选择进行该网站木马检查任务的站点，可选择多个站点。

检查方式：选择沙箱和静态检测方式中一种。

检测深度：设置该网站木马检查任务的检测深度。

检测周期：可选择立即执行，每 N 分钟执行一次，每 N 小时执行一次，定时执行，每天执行一次，每周执行一次，每月执行一次。

选择报警组：选择告警默认模板或自定义模板。

图 2.1.2-27 新增网站木马检查任务

2.1.2.4.8 网站钓鱼检测

WEBUI：主界面 -> 任务中心 -> 任务管理 -> 网站钓鱼检测

钓鱼检查：非法分子的钓鱼网站可能损害用户的财产名誉安全，所以要检测。

可支持 ipv6 地址的检测。通过高级检索按照任务名称和站点名称进行查询。

图 2.1.2-28 网站钓鱼检查

检测名称：填写网站钓鱼检测任务的名称

站点选择：选择进行网站钓鱼检测任务的站点

检测周期：可选择立即执行，每 N 分钟执行一次，每 N 小时执行一次，定时执行，每天执行一次，每周执行一次，每月执行一次。

页面相似度:默认显示 50%的页面相似度,可选择该下拉框中的 25%,50%,75%，100%其中一个页面相似度。

引擎选择：默认选择百度引擎和 Google 引擎，也可直接输入其他的引擎名称。

选择报警组：可选择告警默认模板或自定义的告警模板。

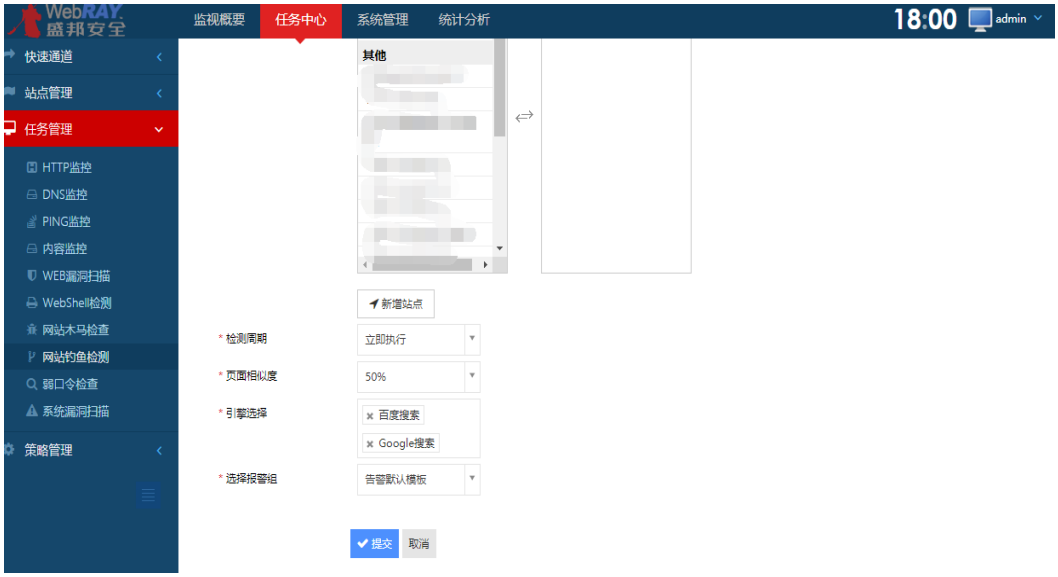


图 2.1.2-29 新增网站钓鱼检测

2.1.2.4.9 弱口令检查

WEBUI：主界面 -> 任务中心 -> 任务管理 -> 弱口令检查

弱口令检查：弱口令指的是仅包含简单数字和字母的口令，例如“123”、“abc”等，因为这样的口令很容易被别人破解，从而使用户的计算机面临风险，所以要检测。通过 superman 账户开启 web 弱口令，可建立 http-get、http-post、https-get、https-post 这四种弱口令任务。可支持 ipv6 地址的弱

口令检查。

高级检索：可根据任务名称，站点名称，模板类型进行查询。

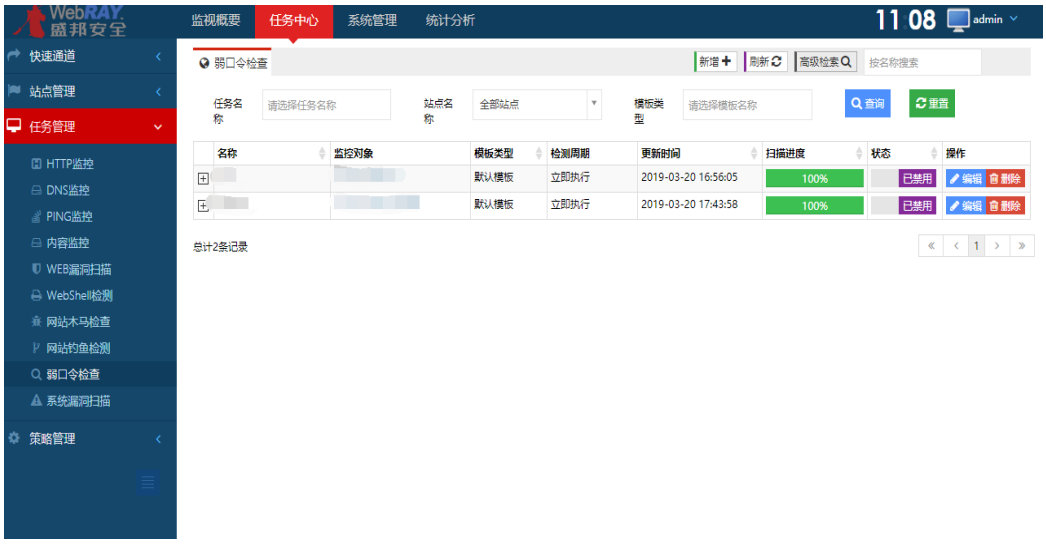


图 2.1.2-30 弱口令检查

任务名称：填写该 http 弱口令任务的名称。

站点选择：选择进行该 http 弱口令任务的站点

检测周期：可选择立即执行，每 N 分钟执行一次，每 N 小时执行一次，定时执行，每天执行一次，每周执行一次，每月执行一次。

服务类型：选择 http-get、https-get、http-post、https-post 四种服务类型中的一种，若选择自定义的 http 类型字典，通过 superman 账户中系统管理-》系统规则管理-》弱口令规则管理上传自定义的相关 http 类型字典。注意：http 弱口令任务支持一个站点，不支持多个站点的 http 弱口令任务。参数的填写方式可参考参数说明。

数据库类型：可选择 mysql、postgres、mssql 等数据库类型，支持选择多个数据库类型。

选择告警组：可选择告警默认模板。

图 2.1.2-31 新增 http 弱口令检查任务

2.1.2.4.10 系统漏洞扫描

WEBUI：主界面 -> 任务中心 -> 任务管理 ->系统漏洞扫描

弱口令检查：弱口令指的是仅包含简单数字和字母的口令，例如“123”、“abc”等，因为这样的口令很容易被别人破解，从而使用户的计算机面临风险，所以要检测。可支持 ipv6 地址的系统漏洞扫描。

图 2.1.2-32 系统漏洞扫描

监控名称：填写该系统漏洞扫描任务的名称。

站点选择：选择进行该系统漏洞扫描任务的站点，可选择多个站点。

选择报警组：可选择告警默认模板或自定义告警模板。

检测周期：可选择立即执行，每 N 分钟执行一次，每 N 小时执行一次，定时执行，每天执行一次，每周执行一次，每月执行一次。

图 2.1.2-33 新增系统漏洞扫描

2.1.3 系统管理

2.1.3.1 用户管理

WEBUI：主界面 -> 系统管理 -> 用户管理 -> 用户管理

二级用户可登陆新建三级用户并加以管理：

图 2.1.3-1 用户管理

系统管理-》用户管理-》用户管理，可通过手机号获取验证码并新增用户。

用户名：创建的用户名即为密码。

权限模板：可选择默认组用户例外菜单，如果为空，可添加自定义模板。

站点数上限：设置该账户可使用的最大站点数。

所属地区：设置该用户的地区。

账户类型：设置该用户为测试用户，试用用户，正式用户。

短信告警条数：设置该用户的最大短信告警条数。

到期时间：填写该用户的到期时间。

登录超时时间：设置该用户的登录超时时间，

E-mail：填写该用户的 E-mail，可用于接收告警邮件。

手机号：填写该用户的手机号，用于对该手机号发送短信告警。注意：需要先在 superman 账户下短信配置里填写短信配置信息。

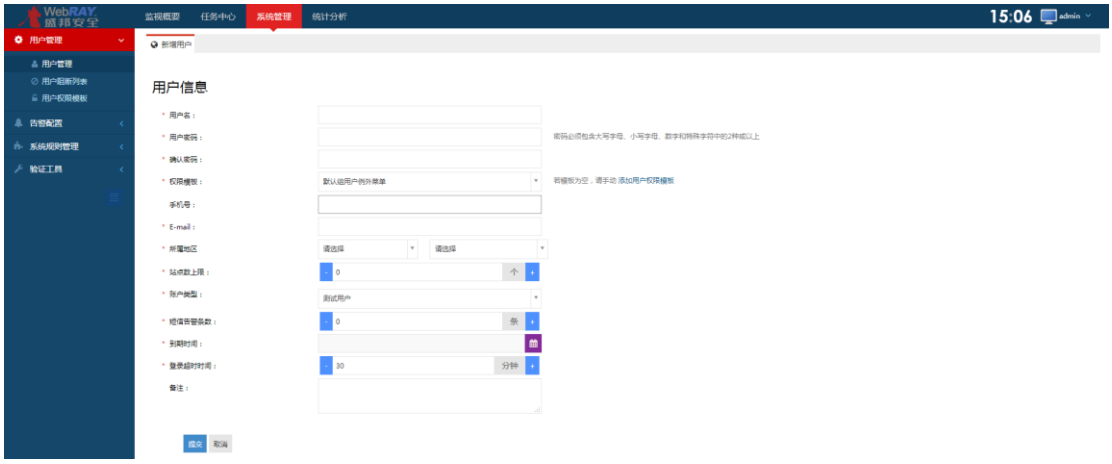


图 2.1.3-2 新增用户

2.1.3.2 用户信息中心

WEBUI：主界面 -> 系统管理 -> 用户管理 -> 用户信息中心

用户信息中心：通过添加姓名、旧密码、新密码、确认密码、电话、E-mail，来修改用户配置信息。默认的二级用户可以修改电话，邮箱，其他默认不可修改。

图 2.1.3-3 个人信息配置

2.1.3.3 用户阻断列表

WEBUI：主界面 -> 系统管理 -> 用户管理 -> 个人信息配置

用户阻断列表显示配置：用户连续尝试 5 次登陆失败则会被加入阻断列表并详细到被阻断用户的登陆名，来源 ip、阻断时间。用户阻断列表即用户被锁定，可通过上级用户解除阻断。即如下图所示，admin 账户属于二级用户，需要上级用户 superman 来给 admin 账户解除锁定。解除后用户阻断列表就没有该用户被阻断的记录。

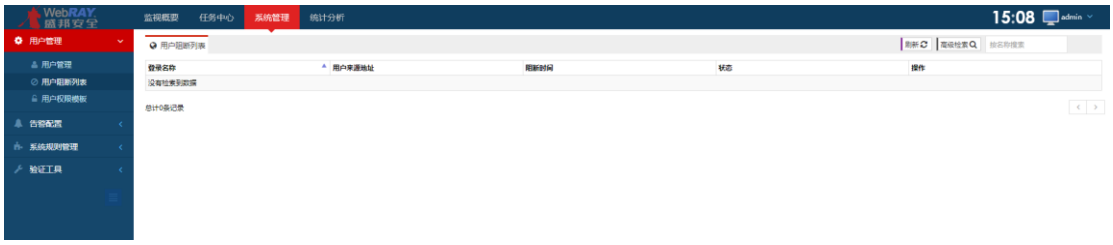


图 2.1.3-4 用户阻断列表

2.1.3.4 用户权限模板

WEBUI：主界面 -> 系统管理 -> 用户管理 -> 用户权限模板

用户权限模板配置：通过例外对应权限可生成自定义模板，并应用于用户方便管理。

图 2.1.3-5 用户权限模板

WEBUI：主界面 -> 系统管理 -> 用户管理 -> 用户权限模板

选择新增一用户权限模板：

模板名称：填写所建立的模板名称。

例外功能点：一旦被例外的功能，模板中就不会出现这个功能。

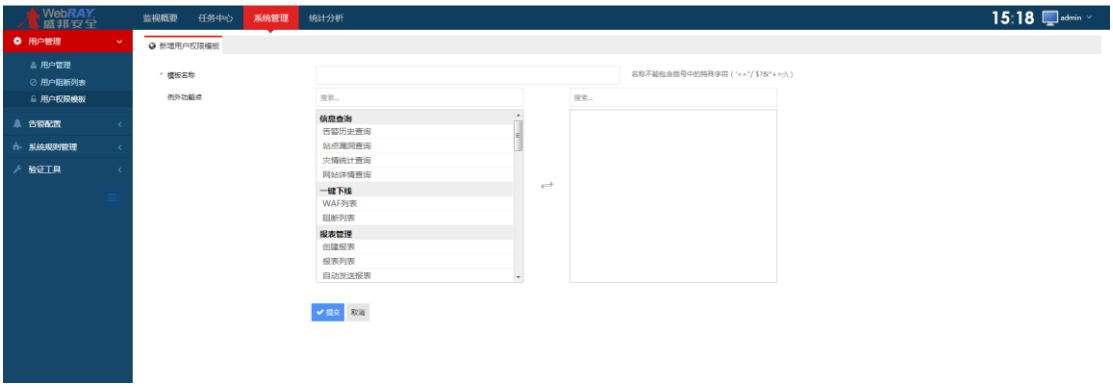


图 2.1.3-6 新增用户权限模板

2.1.3.5 告警配置

WEBUI：主界面 -> 系统管理 -> 告警配置

告警接收人管理：新增、编辑和删除告警接收人；告警接收人信息包括姓名、

电话、E-Mail、微信。

告警组管理：新增、编辑和删除告警组；可对告警方式、告警类型等信息和告警时段进行配置，并关联告警接收人。

2.1.3.5.1 告警组管理

WEBUI：主界面 -> 系统管理 -> 告警配置 -> 告警组管理

新增告警组：点击“新增”按钮进入详情页面，根据提示输入和选择对应信息。

报警组名称：填写告警组名称。

描述：填写告警组描述。

微信告警：选择开启/关闭微信告警，添加微信公众号，可获取微信告警信息。

邮件报警：选择开启/关闭邮件告警，关联告警联系人的 E-mail 邮箱。

短信报警：选择开启/关闭短信告警，关联告警联系人的电话（手机）。

告警类型：包括 HTTP 监控、DNS 监控、PING 监控、内容监控、WEB 漏洞扫描、弱口令扫描等，根据需要勾选告警的任务类型。建议：不要勾选太多内容，过多的告警信息将造成告警冗余，不利于管理员监视网站安全动态。

短信接收时段：选择短信告警接受时段，从 0-24 时，可通过条形选择框或手动输入来设置。

关联报警接收人：关联已添加的报警接收人。

点击“提交”按钮完整告警联系人信息配置，告警组管理列表查看已添加的告警组并且可进行编辑和删除操作。监控平台默认已有一个告警组，如果配置信

息不多，可直接对默认告警组进行编辑使用。

图 2.1.3-7 告警组管理

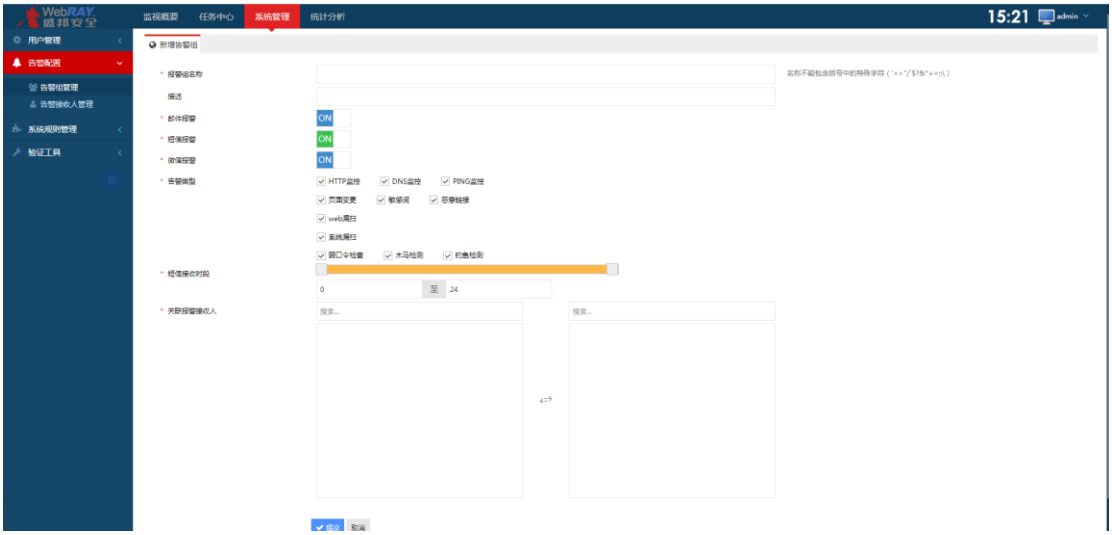


图 2.1.3-8 新增告警组

2.1.3.5.2 告警接收人管理

WEBUI：主界面 -> 系统管理 -> 告警配置 -> 告警接收人管理

新增告警接收人：点击“新增”按钮进入详情页面，根据提示输入和选择对应信息。

姓名：告警接收人姓名。

电话：告警接收人电话（请填写手机号码，用于短信报警）。

E-mail：告警接收人 E-mail（请保证邮箱畅通）。

微信号：告警接收人微信（先添加微信公众号）。

点击“提交”按钮完整告警接收人信息配置，告警接收人管理列表查看已添加的告警接收人并且可进行编辑和删除操作。

图 2.1.3-9 接收人管理

图 2.1.3-10 新增接收人信息

2.1.3.6 系统规则管理

WEBUI：主界面 -> 系统管理 ->系统规则管理

系统规则管理包括以下三类：敏感词管理，信任域名管理，弱口令规则管理。

2.1.3.6.1 站点类别管理

WEBUI：主界面 -> 系统管理 ->系统规则管理 -> 站点类别管理

监控平台站点类别管理是为了方便用户的分类、整理和查找用户站点而设，并支持添加自定义站点类别。

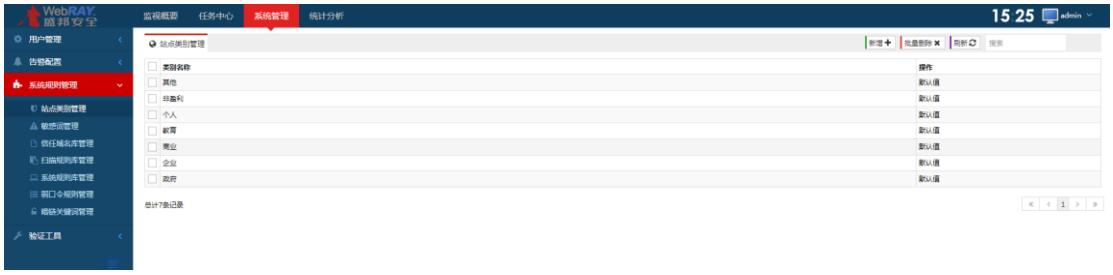


图 2.1.3-11 站点类别管理

输入站点类别，即自定义站点类别名称。

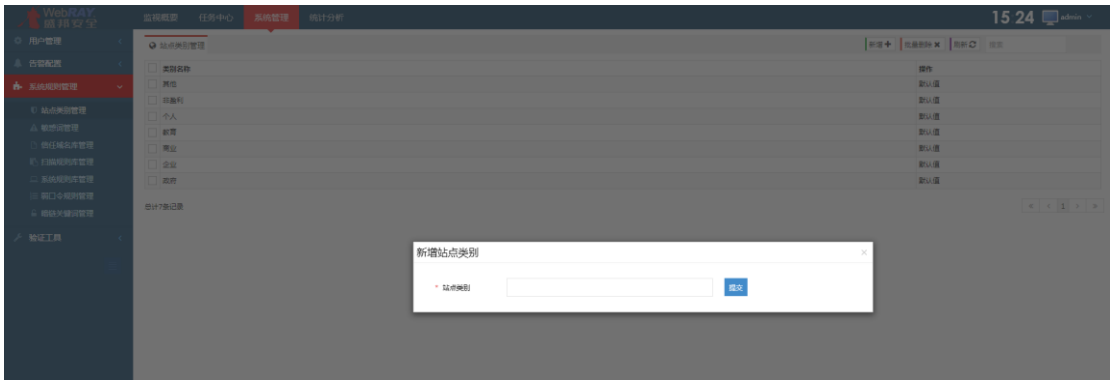


图 2.1.3-12 新增站点类别

2.1.3.6.2 敏感词管理

WEBUI：主界面 -> 系统管理 ->系统规则管理 -> 敏感词管理

监控平台内置海量敏感词库，并且支持用户添加自定义敏感词，全部敏感词信息在列表中展现，默认敏感词库不支持编辑和删除操作。

添加自定义敏感词：添加可选择单个域名添加和批量添加。

单个敏感词添加：点击“新增”按钮，进入新增敏感词页面，按照提示输入并选择敏感词，敏感词类别，风险等级。

批量添加：点击“导入”按钮，下载模版（KeywordTempletx.xls），按照模版格式填写所要添加的敏感词，保存后上传，完成批量添加。

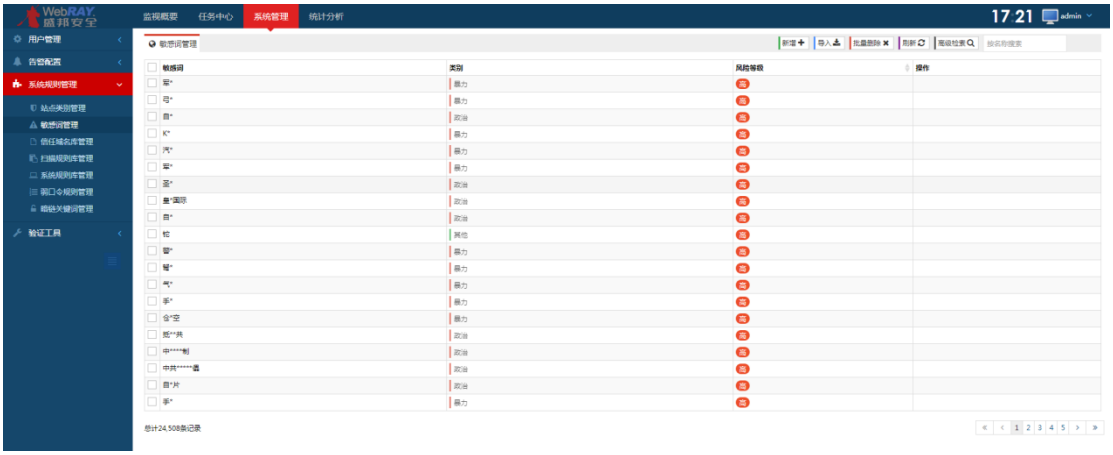


图 2.1.3-13 敏感词管理

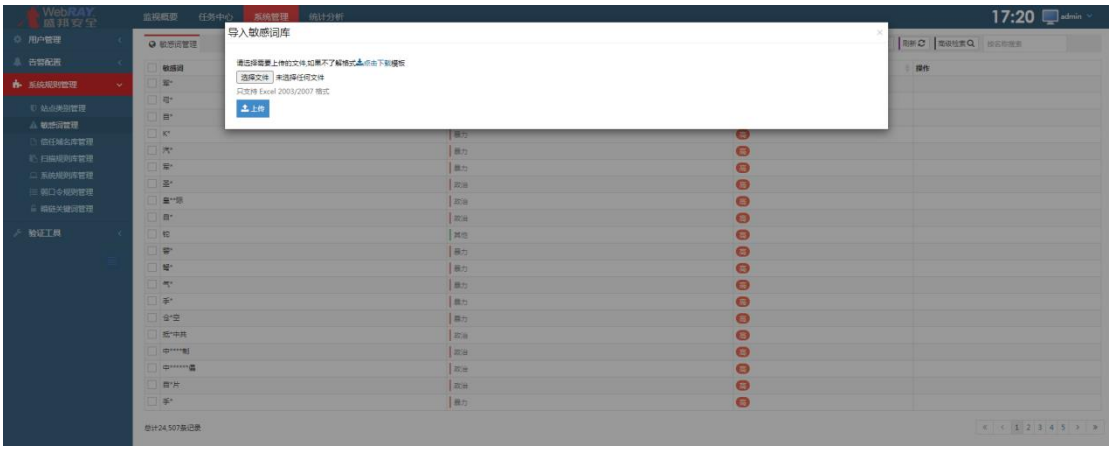


图 2.1.3-14 导入敏感词库

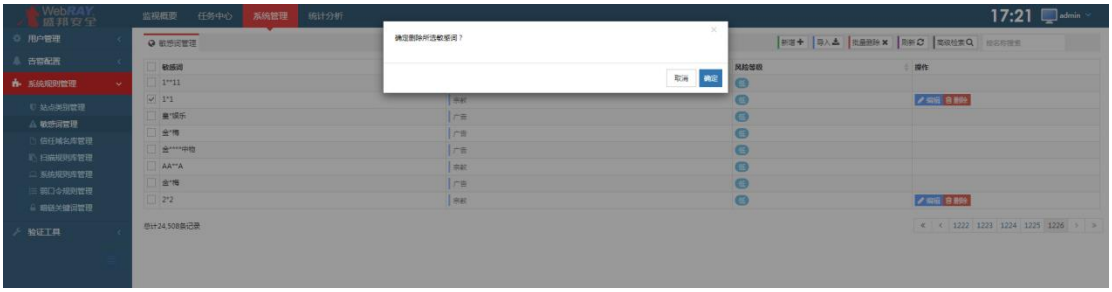


图 2.1.3-15 批量删除敏感词

2.1.3.6.3 信任域名库管理

WEBUI：主界面 -> 系统管理 ->系统规则管理 -> 信任域名库管理

用户可根据需要添加信任域名，信任域名将会被监控平台视为安全域名，从而降低报警。

单个域名添加：点击“新增”按钮，进入新增域名页面，按照提示信任域名和描述。

图 2.1.3-16 信任域名库

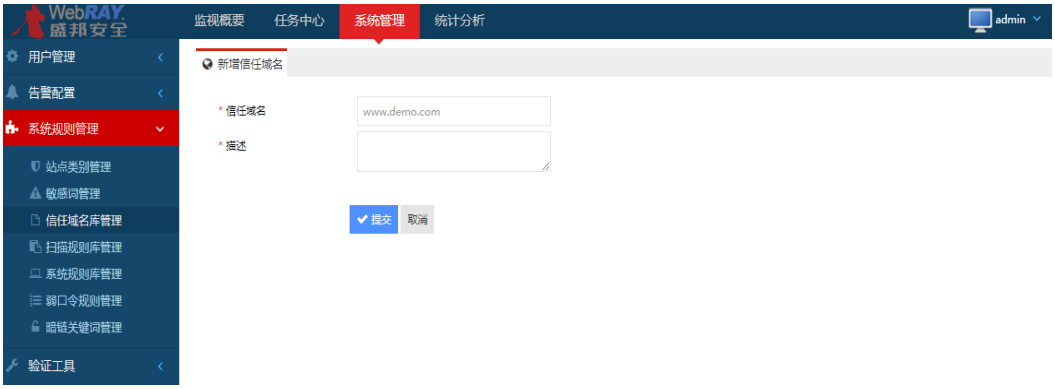


图 2.1.3-17 新增信任域名

2.1.3.6.4 扫描规则库管理

WEBUI：主界面 -> 系统管理 ->系统规则管理 -> 扫描规则库管理

用户可在此处按照漏洞名称、分类和漏洞级别来查询扫描 web 漏洞的所用规则库文件，规则库会持续更新，敬请及时关注规则库升级情况并加以更新，以获得最新规则库不遗漏相关漏洞信息。

图 2.1.3-18 扫描规则库

2.1.3.6.5 弱口令规则管理

WEBUI：主界面 -> 系统管理 ->系统规则管理 -> 弱口令规则管理

弱口令规则管理中，用户可根据自身需求添加常用的用户名，监控平台内置海量弱口令字典，扫描时引擎将对常用用户名和弱口令字典进行排列组合，查找网站中存在的弱口令。上传字典时可选择 http 弱口令类型的字典上传。若上传不了，先确认 superman 账户是否开启这个 web 弱口令。

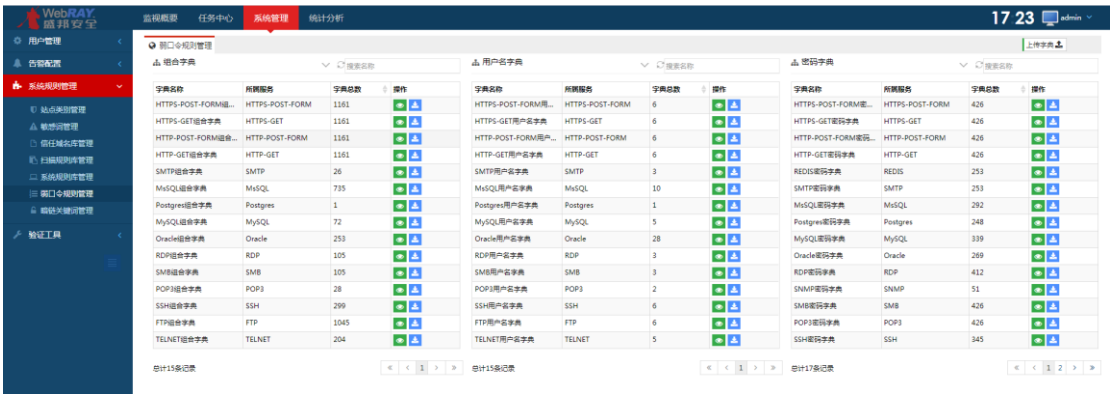


图 2.1.3-19 弱口令规则

2.1.3.6.6 系统规则库管理

WEBUI：主界面 -> 系统管理 ->系统规则管理 -> 系统规则库管理

用户可在此处按照漏洞名称、分类和漏洞级别来查询扫描系统漏洞的所用规则库文件，规则库会持续更新，敬请及时关注规则库升级情况并加以更新，以获得最新规则库不遗漏相关漏洞信息。

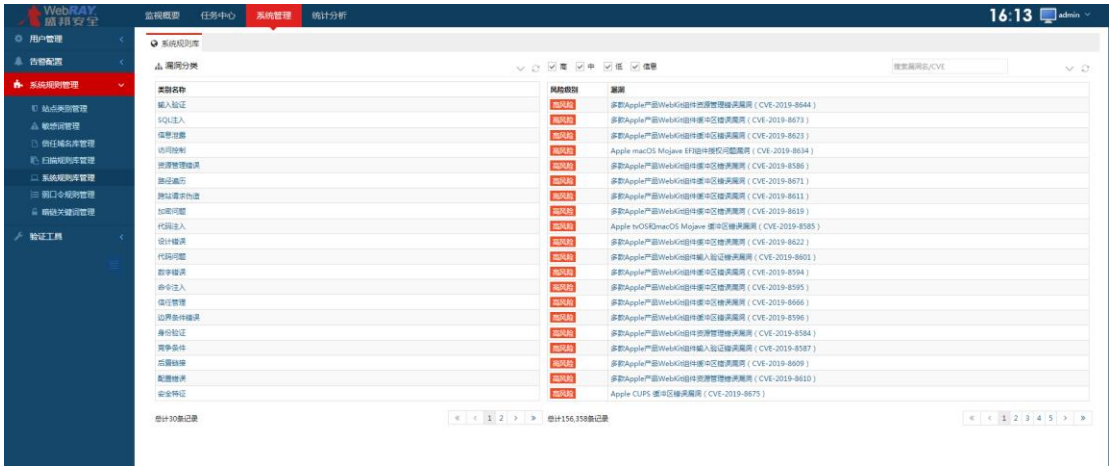


图 2.1.3-20 系统规则库

2.1.3.6.7 暗链关键词管理

WEBUI：主界面 -> 系统管理 ->系统规则管理 -> 暗链关键词管理

监控平台内置暗链关键词词库，并且支持用户添加自定义暗链关键词，全部暗链关键词信息在列表中展现，默认敏感词库不支持编辑和删除操作。

添加自定义暗链关键词：单个暗链关键词添加：点击“新增”按钮，进入新增敏感词页面，按照提示输入暗链关键词和描述。

批量删除：可对一个或多个的暗链关键词进行删除，提高删除的效率。

图 2.1.3-21 暗链关键词管理

2.1.3.7 验证工具

WEBUI：主界面 -> 系统管理 -> 验证工具

漏洞验证工具包括以下两类：通用验证工具和 SQL 注入验证工具。

2.1.3.7.1 通用验证

WEBUI：主界面 -> 系统管理 -> 验证工具 -> 通用验证工具

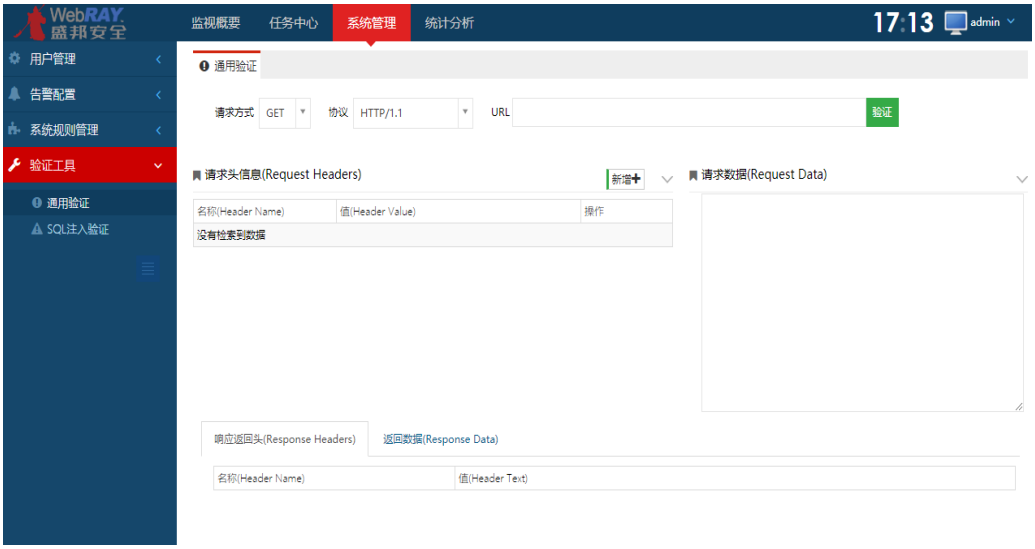


图 2.1.3-22 通用验证

2.1.3.7.2 SQL 注入验证

WEBUI：主界面 -> 系统管理 -> 验证工具 -> SQL 注入验证工具

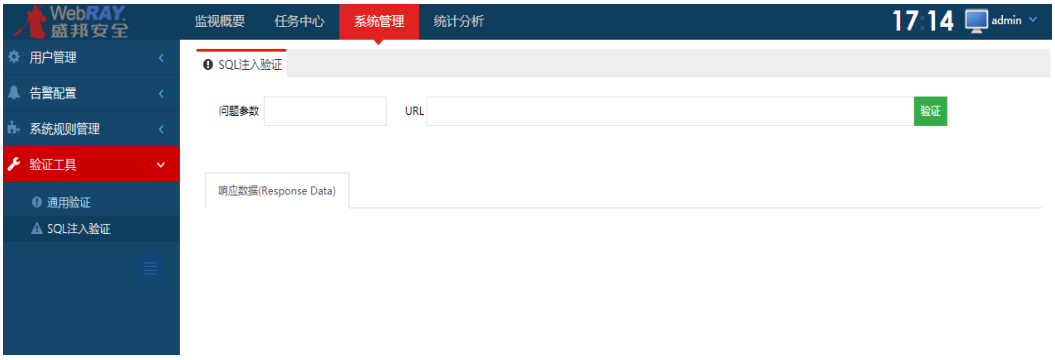


图 2.1.3-23 SQL 注入验证

2.1.4 统计分析

2.1.4.1 数据分析

2.1.4.1.1 漏洞分析

WEBUI：主界面 -> 统计分析 ->数据分析->漏洞分析

根据漏洞类型、风险等级、漏洞名称、目标漏洞进行检索。检索到的结果会在右边显示出详细的漏洞信息，根据检索到的漏洞显示漏洞行业分布、漏洞地区分布、漏洞系统分布、漏洞用户分布、漏洞站点分布。全局显示该漏洞的整体情况。

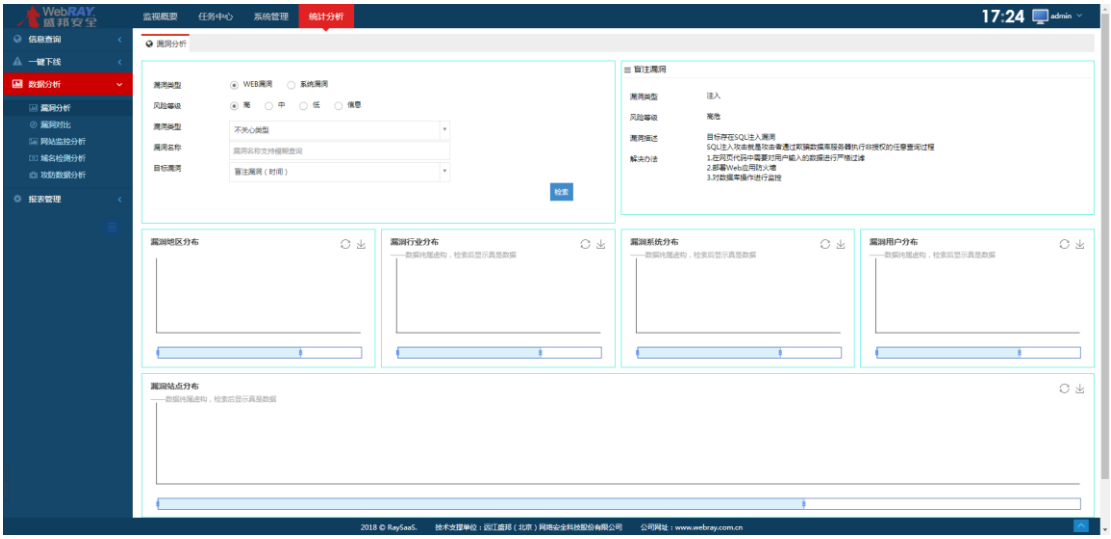


图 2.1.4-1 漏洞分析

2.4.1.2 网站监控分析

WEBUI：主界面 -> 统计分析 ->日志中心 -> 网站监控分析

网站监控分析页面选择监测类型（HTTP，DNS，PING，篡改，暗链，敏感词），选择监测任务，时间范围和监测点，点击“查询”按钮完成查询。查询内容以图表方式显示在下方列表中。

图 2.1.4-2 网站监控分析

2.4.1.3 域名检测分析

WEBUI：主界面 -> 统计分析 ->日志中心 -> 域名检测分析

域名检测分析页面选择检测类型（WEB 漏洞扫描，弱口令检查），选择检测任务和最近扫描次数，点击“查询”按钮完成查询。查询内容以图表方式显示在下方列表中。

图 2.1.4-3 域名检测分析

2.4.1.4 攻防数据分析

WEBUI：主界面 -> 统计分析 ->数据分析 -> 攻防数据分析

域名检测分析页面选择攻击类型（WAF，DOOS），选择目标地址、攻击源地址和目的端口，点击“查询”按钮完成查询。查询内容以图表方式显示在下方列表中。

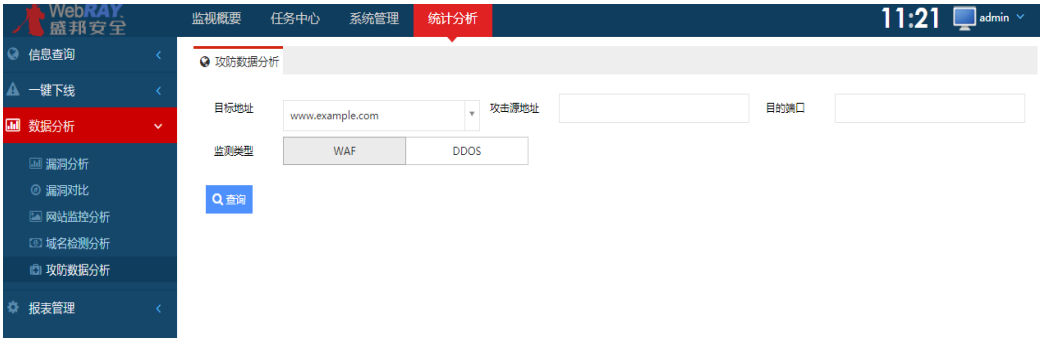


图 2.1.4-4 域名检测分析

2.4.1.5 漏洞对比

WEBUI：主界面 -> 统计分析 ->数据分析 -> 漏洞对比

目标站点：选择要对比的站点名称，可通过站点名称，url，网站类型，网站标签，所属标签，存在漏洞，漏洞等级来筛选站点。

漏洞类型：选择要对比的漏洞类型，web 漏洞或系统漏洞。

对比任务：选择该站点的不同任务 ID 号，该站点如果被执行过两次，就可以进行漏洞对比，选择其中一个任务 ID 号作为整改前的任务，另一个任务 ID 号为整改后的任务进行对比。对比两个任务中漏洞数量和新增漏洞的变化，以饼形图和柱形图形式生动形象的展示出来。

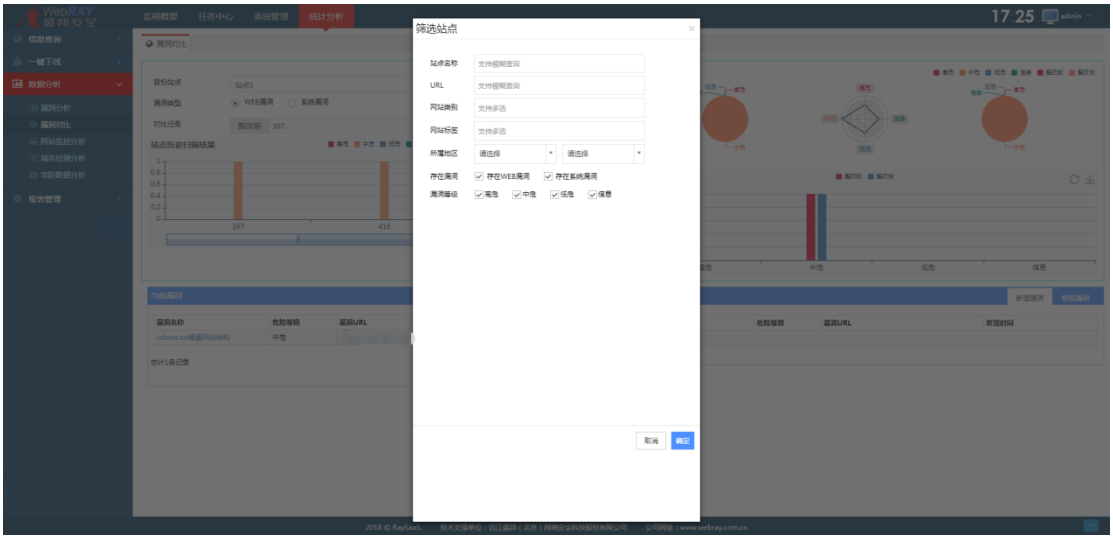


图 2.1.4-5 筛选站点名称

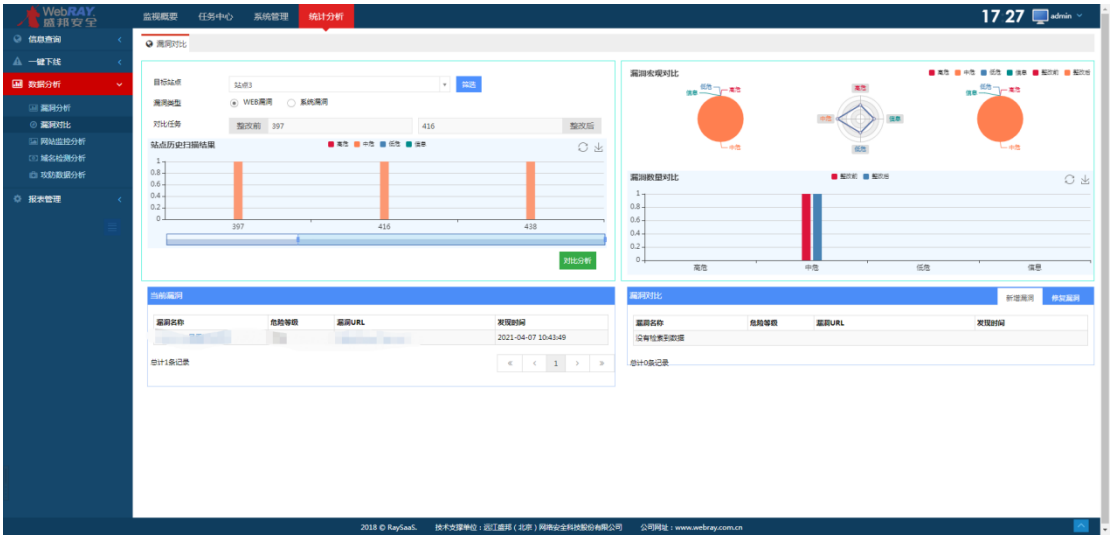


图 2.1.4-6 漏洞对比

2.1.4.2 信息查询

2.1.4.2.1 网站详情查询

WEBUI：主界面 -> 统计分析 -> 信息查询 -> 网站详情查询

网站详情查询中可以查看网站的详细情况，并给出打分值。展开查询，可以查看网站存在的详细漏洞情况。

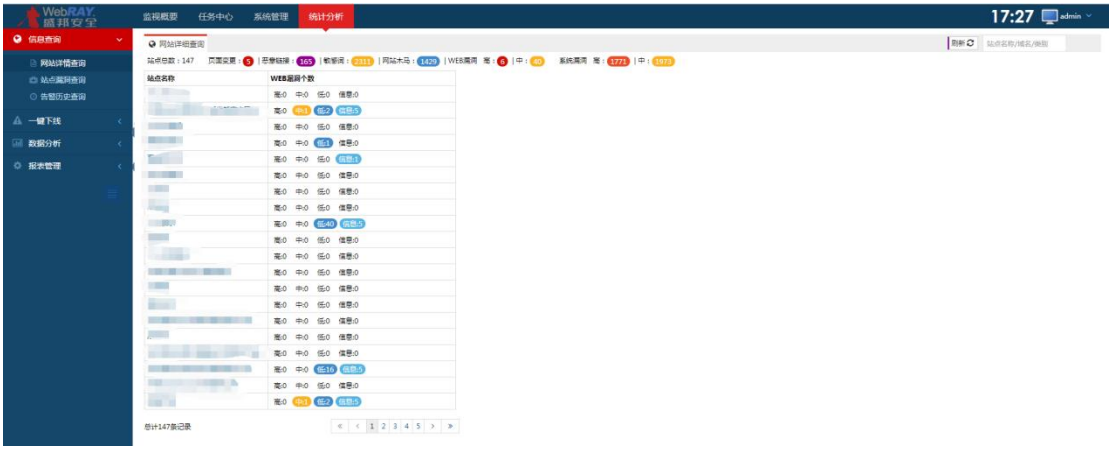


图 2.1.4-7 网站详情查询

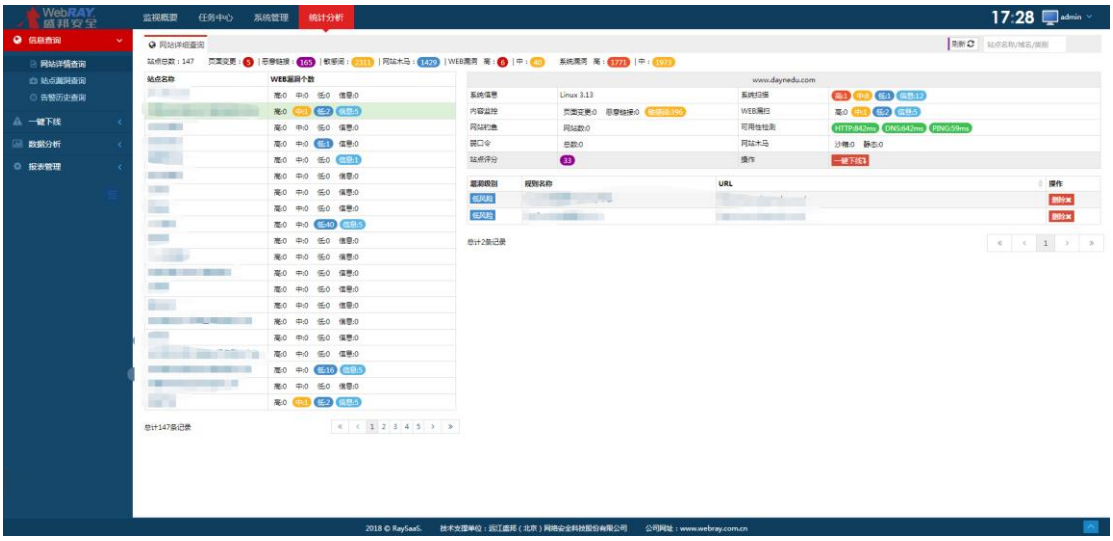


图 2.1.4-8 网站详细查询展开页面

2.1.4.2.2 告警历史查询

WEBUI：主界面 -> 统计分析 ->信息查询 -> 告警历史查询

告警历史查询页面选择任务类别（全部类别，HTTP 监控，DNS 监控，PING 监控，内容监控，WEB 漏洞扫描，弱口令检查），选择时间范围，点击“查询”按钮完成查询。查询内容显示以表格方式在下方列表中。其中高级检索可按日期范围、监控对象名称、接收人、选择类别来查询该菜单中告警历史。

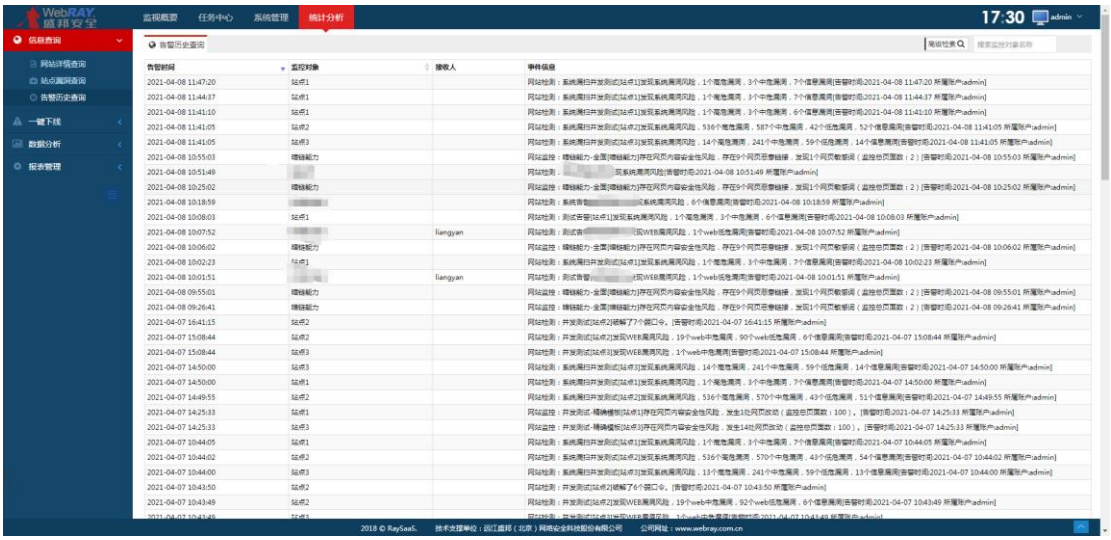


图 2.1.4-9 告警历史查询

2.1.4.2.3 站点漏洞查询

WEBUI：主界面 -> 统计分析 ->信息查询-> 站点漏洞查询

站点统计查询可以查看网站的 web 漏洞和系统漏洞不同危险等级情况，以及所属类别和对应评分。还可提供站点删除和导出具体报表的服务。通过该页面的高级检索功能，可以按站点名称、评分范围、类别来进行查询。

人工研判功能主要是在勾选该页面的一站点后出现人工研判的按钮实现功能。人工研判可以对勾选的站点对内容监控，web 漏洞扫描、网站木马检测、

弱口令检测、网站钓鱼检测、系统漏洞检测这些检测结果进行确认或删除，以及截图。

批量删除功能：在点击该站点的系统漏洞数字、web 漏洞数字、恶意链接、内容监控数字后，页面会显示批量删除按钮，勾选全选框可进行批量删除操作。

图 2.1.4-10 站点漏洞查询

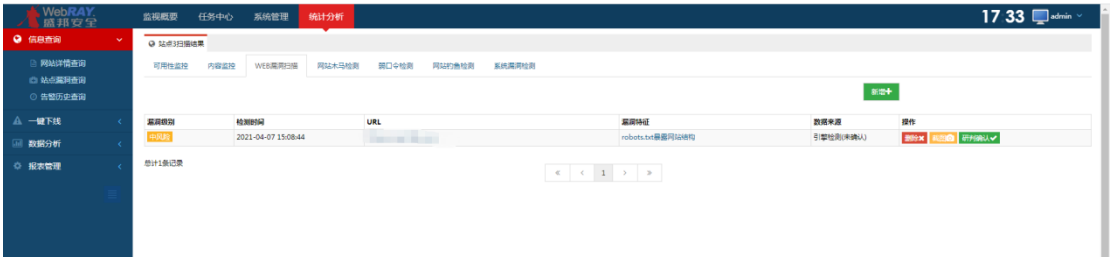


图 2.1.4-11 人工研判界面

2.1.4.3 报表管理

2.1.4.3.1 创建报表

WEBUI：主界面 -> 统计分析 -> 报表管理 -> 创建报表

创建报表功能提供四种类型报表供用户选择，导出报表会有进度条显示导出进度。

详细报表：此报表针对各站点生成详细报表格式，包含了系统漏洞风险统计、

web 漏洞风险统计、以及具体漏洞数据等。

统计报表：此报表适用于监管人员，用于分析一段时间内总体安全态势、安全趋势与安全工作量，便于迅速分析问题所在，有助于做出正确的安全决策。

检测报告：此报表适用于管理人员，对批量网站一键生成数据表格，用于对安全决策做数据支撑，也可用作对各单位安全情况作通告。

任务报告：此报表适用于含有特殊要求的公安人员的定制报告。

站点选择：左侧栏内列出已添加的站点，点击后站点转移到右侧栏内，完成选择。

标签选择：可按照标签在站点列表中搜索对应站点。

地区选择：可按照地区在站点列表中搜索对应站点。

快速导出：开启“快速导出” 开关后报表中将不生成图片，提高导出效率。

可用性监控：勾选 HTTP 监控、DNS 监控、PING 监控中的一个或多个，可用性监控默认为 24 小时内数据，导出为可用性产生告警的数据时间点。

自定义日期：自定义日期，获取这个日期范围内所选择的任务数据，自定义日期仅针对安全性和合规性结果。

内容监控：可勾选页面变更、恶意链接、敏感词中的一个或多个。

检测类型：选择要导出的任务信息，包括 WEB 漏洞、弱口令、钓鱼、

WAF 防护：可勾选 WAF 防护，获取 WAF 防护的数据信息存在于报告中。

导出格式：在详细报告和统计报告中，导出格式可分为 HTML 格式、XML 格式、WORD 格式、PDF 格式

报表名称：填写报表名称。

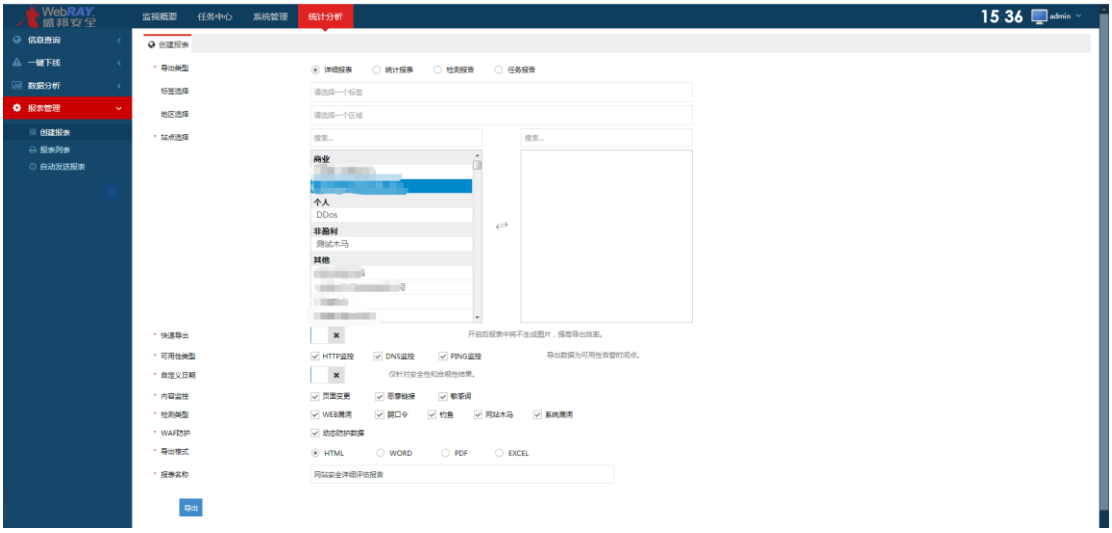


图 2.1.4-13 详细报表

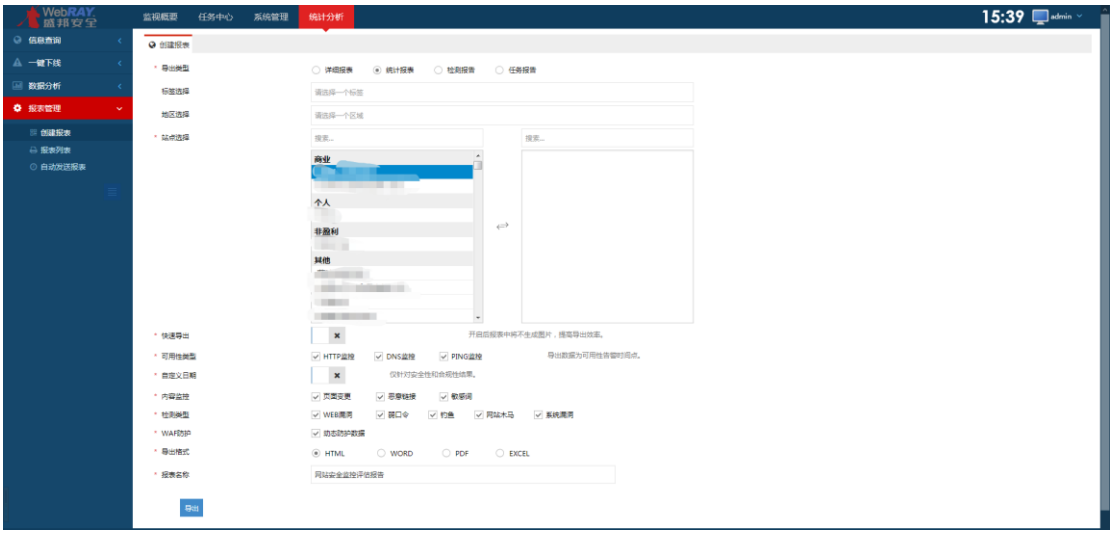


图 2.1.4-14 统计报表

图 2.1.4-15 检测报表

图 2.1.4-16 任务报表

2.1.4.3.2 报表列表

WEBUI：主界面 -> 统计分析 -> 报表管理 -> 报表列表

报表列表中可查看已经生成的报告。

图 2.1.4-17 报表列表

2.1.4.3.3 自动发送报表

WEBUI：主界面 -> 统计分析 -> 报表管理 -> 自动发送报表

自动发送周报生成的报表到指定的邮箱。通过高级检索按照

图 2.1.4-18 自动发送报告

图 2.1.4-19 新增一自动发送周报

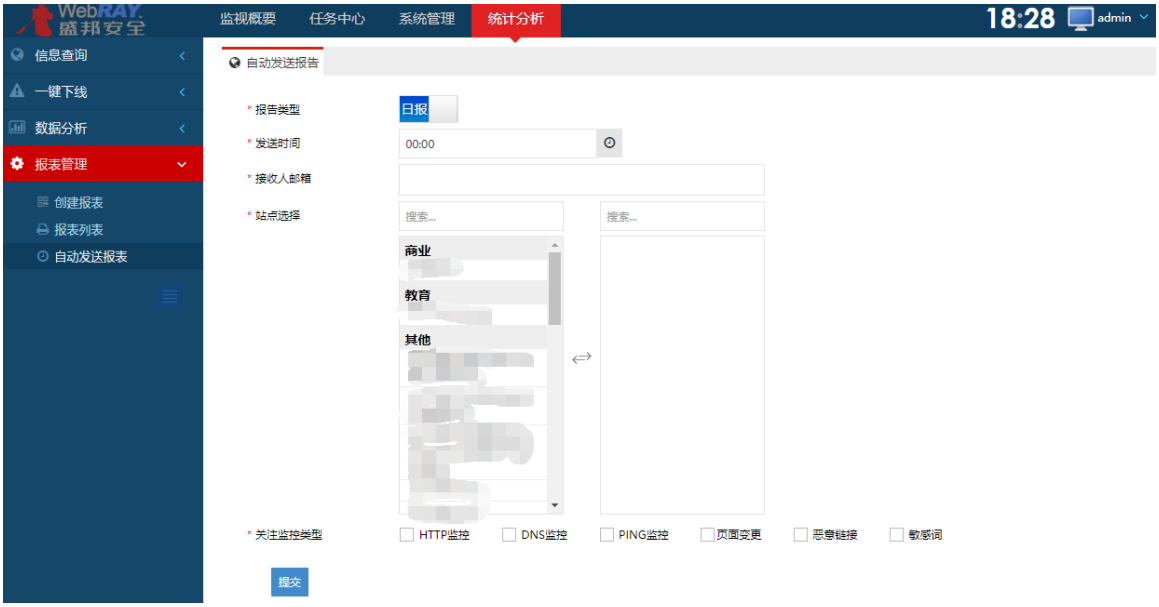


图 2.1.4-20 新增一自动发送日报

2.1.4.4 一键下线

WEBUI：主界面 -> 统计分析 -> 一键下线

2.1.4.4.1 WAF 列表

WEBUI：主界面 -> 统计分析 -> 一键下线 -> WAF 列表

在 WAF 列表中配置 WAF 名称、WAF 地址、防护域名、要实现防护的 WAF 账户和 WAF 的防护范围实现防护环境的配置工作。注意：要实现 WAF 防护功能须 WAF 串联在网络环境内，可参考测试网络拓扑图。可通过高级检索按照 WAF 名称、WAF 地址、WAF 账户筛选条件进行查询搜索。

图 2.1.4-21 waf 列表

2.1.4.4.2 阻断列表

WEBUI：主界面 -> 统计分析 -> 一键下线 -> 阻断列表

在 WAF 列表中配置成功并实现正常实现防护的站点会同步到阻断列表中，并支持对已阻断列表的批量上线。

图 2.1.4-22 阻断列表