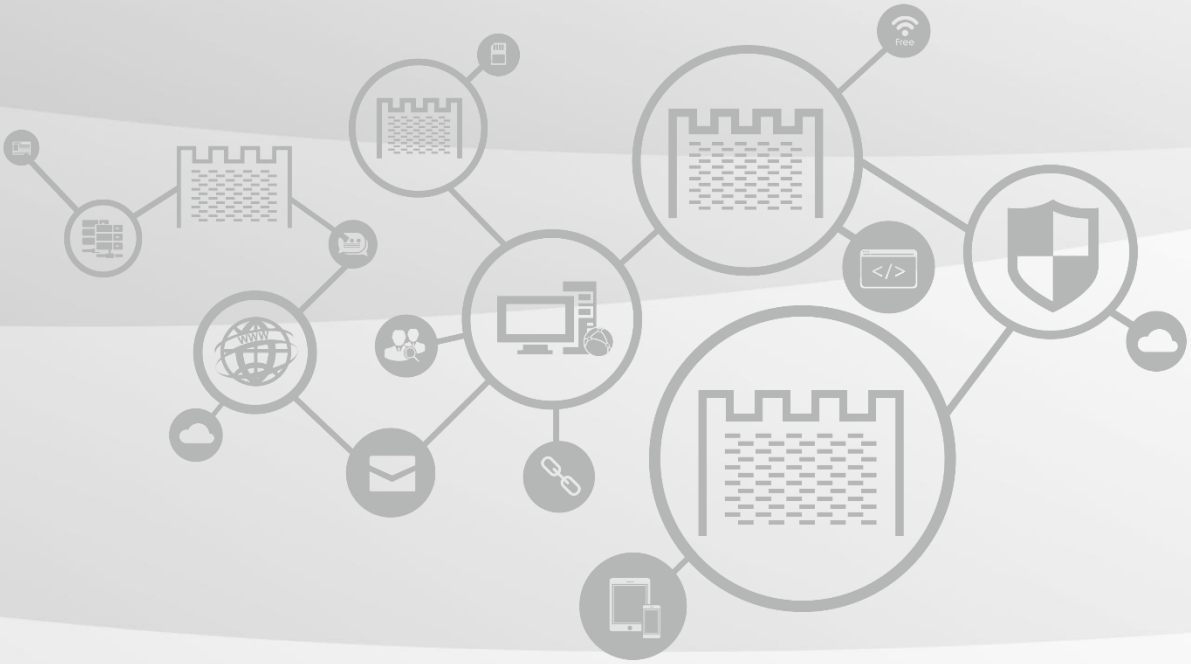
RayScan 一体化漏洞评估系统

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

■ 版权声明

目录

前言

文档范围

本文详细介绍了 RayScan 一体化漏洞评估系统 V3.0（以下简称为漏扫）的 Web 管理界面的所有功能特点及使用方法。

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

内容简介

产品概述	介绍漏扫的产品特点。
基础配置向导	介绍漏扫的连接方式和界面风格。
系统整体概述	介绍系统用户、页面布局以及功能
简介版任务页面	介绍简介版任务页面详情
许可证管理	介绍授权相关信息
任务中心	介绍系统扫描、Web 扫描任务、未知站点、安全基线核查等相关任务的下发配置、扫描详情、漏洞详情展示
资产管理	介绍系统扫描、Web 扫描资产的管理以及扫描漏洞详情展示
策略模板	介绍任务扫描时相关漏洞插件配置

报表管理	介绍任务相关漏洞的报表导出
系统管理	介绍网络配置、升级等相关系统管理
审计日志	介绍设计管理员的相关日志操作
附录：出厂参数	介绍漏扫的出厂默认配置

获得帮助

如需获取网络安全相关资料，请访问网站：http://www.webray.com.cn/

如需获取更详尽网络安全专业服务信息、商务信息，您可通过如下方式与我们联系：

咨询热线：400-6911-199

总机：+86 10 8273 0576

传真：+86 10 8273 0577

Email： info#webray.com.cn

格式约定

粗体字 —— 命令和关键字

——使用技巧、建议和引用信息等

——重要信息

【XXX】—— 按键名称的表示方式

A -> B —— 菜单项选择的表示方式

注：本文中所有图例均为屏幕截取。

1. 产品概述

1.1.背景

在当前的信息技术时代，实时地了解信息系统面临的安全风险对所有的安全管理员来说都越来越重要，而风险管理中脆弱性管理尤为重要，已经成为标准的核心要素，漏洞扫描产品正是实现漏洞自动化管理的工具，它可以帮助信息系统管理人员随时掌握当前系统中漏洞情况。

脆弱性管理是主动防御的思维的一种体现，即通过提前降低整个系统的可攻击弱点，来减少被攻击风险的一种安全思维模式。系统脆弱性主要来自两个方面，一方面是系统存在未修补的漏洞，另一方面是系统配置存在风险如开放了不必要的远程端口和服务。

随着业务系统增多，脆弱性管理的重要性和难度也都相应增加，一方面由于业务系统的集中部署，客观上存在着短板效应，即只要突破一个最薄弱的系统，就可以利用这个系统对其他主机或应用程序展开更难识别和防御的攻击。另外，系统由多个部门使用，数据中心的管理者并不了解每一个业务系统的具体情况，使得脆弱性管理非常困难。

盛邦安全一体化漏洞评估系统，可通过集中管理、周期性扫描，从多个维度对网络环境中所有系统或网站进行脆弱性扫描和整体评估分析，为网络管理者提供有效的风险评估方法和加固方案。

1.2.体系结构

一体化漏洞扫描系统 RayScan 是架构于自有的 RayOS 网络操作系统之上，

使用基于脚本插件的规则库来对目标系统进行黑盒测试的工具，具体架构如下图1.2-1。

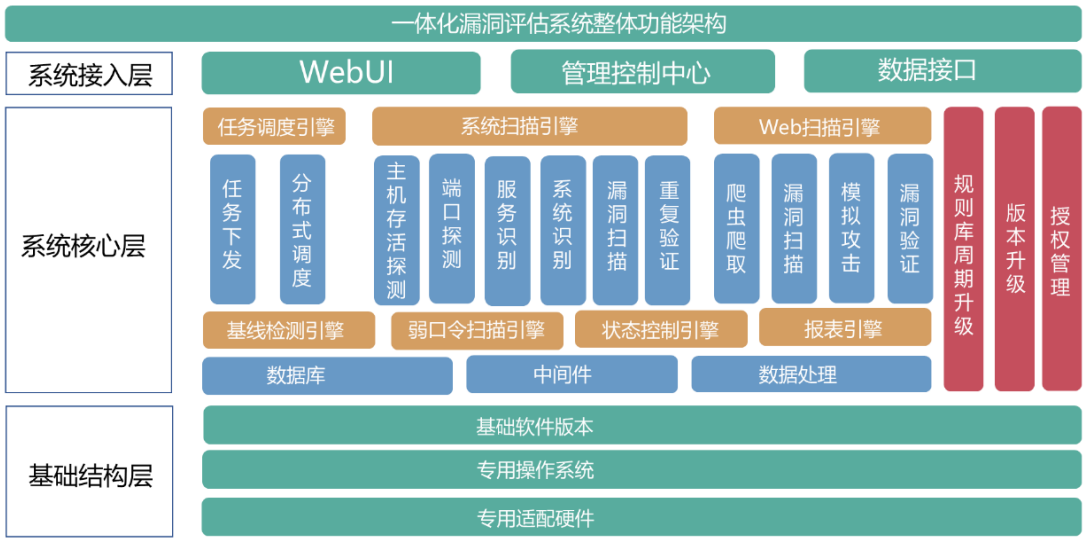


图 1.2-1 一体化漏洞评估系统体系结构

- 任务调度中心

基于负载均衡、指定引擎等多种方式的任务调度模式。

- 插件引擎

高效的插件执行引擎，根据前置条件判断插件是否需要执行，减少多余的测试用例，同时根据端口、服务、版本、认证状况等多种情形提供脚本，检测出尽量多的安全问题，减少漏报。

- 爬虫引擎

用于对 Web 系统的页面获取，支持对 JavaScript、BOM（浏览器对象）、Flash 的解析。

- 端口、服务识别

漏洞扫描的基础模块，采用多种技术手段对端口进行探测，对于服务的识别不仅仅基于端口号，而是发送数据包来对服务器返回数据进行甄别从而判断服务

的类型，大大提高了扫描结果的准确性。

1.3.产品功能介绍

一体化漏洞评估系统产品功能具体介绍见下表 1.3-1 所示：

表 1.3-1 产品功能简介

产品功能	功能说明
系统漏扫	发现网络设备和主机系统的安全漏洞，并提供安全解决建议；可以并行地检查多个被评估的系统，能够提供扫描策略定制，可以保证扫描的安全性，不影响应用系统和网络业务的正常运行
Web 漏扫	发现 Web 站点中的安全漏洞，并提供安全解决建议，对网站 SQL 注入、Cookie 注入、盲注、跨站、文件包含、敏感信息泄露等漏洞进行发现检查
数据库漏扫	数据库系统设置、系统软件本身已知漏洞及系统完整性检查
基线核查	设备的上线安全检查、第三方入网安全检查、合规安全检查、日常安全检查和安全服务任务
口令猜解	多协议、多数据库类型、多组合形式的弱口令扫描
仅基础探测	发现设备是否存活以及设备开放的服务/端口信息

2. 系统整体概述

2.1.概述

Web 管理界面为用户提供了更直观的人机交互方式，用户通过 Web 端登录实现对任务扫描、资产管理、报表导出、系统管理于一体。

本章介绍了一体化漏洞评估系统的基本信息，具体内容如表 2.1-1 所示。

表 2.1-1 管理系统概述

功能	描述
登录系统	介绍登录系统的方法
系统用户	介绍系统用户类型及权限
页面布局	介绍系统页面布局的情况
系统功能介绍	介绍各账号下基本功能模块

2.2.登录系统

登录一体化漏洞评估系统的步骤如下：

- 步骤 1：确认一体化漏洞评估系统的网络连通，即客户端到漏扫的网络可达
- 步骤 2：在如下图所示的页面中填写用户名、密码和验证码进入对应账号下的系统管理界面。

图 2.2-1 登录界面

⚠注意：登录系统注意事项

- 单个账户不支持多个用户同时登录
- 登录失败的原因有可能是：①用户名输入错误 ②密码输入错误 ③验证码填写错误

2.3.页面布局

用户登录后，进入系统当前运行的页面。用户页面布局图如图 2.3-1：

图 2.3-1 系统页面布局

ⓘ：系统页面布局中的主菜单、工作区，显示的内容不同；但在基本信息区显示无差别。

- 主菜单：系统的功能主菜单。
- 工作区：提供系统各个功能的配置、操作和浏览。
- 基本信息：显示硬件使用情况。

⚠：为确保用户账号的安全，建议用户点击【注销】按钮退出系统。

系统功能简介

具体的功能如表 2.3-1 所示。

表 2.3-1 系统功能介绍

菜单		功能
任务中心	新建任务	新建系统扫描、Web 扫描、口令猜解、仅基础探测任务，可对扫描任务进行相关配置
	任务列表	主要显示所有的任务列表以及正在扫描的工作列表
	探测未知站点	主要进行未知站点的扫描，扫描后可转为资产，也可添加为 Web 任务
	安全基线核查	可以对输入的站点进行相关策略规格的核查，可下载核查报告
	数据库检测	可对目标进行数据库漏洞扫描
资产管理	资产管理	展示所有的系统资产以及 Web 资产，可以对资产进行新增、编辑、删除、查询等，也可进行漏洞详情查看
	资产组管理	展示所属用户的资产组，可以进行资产组的新增、编辑、删除等
策略模板	系统插件	展示所有的系统漏洞类别以及漏洞插件，可以对漏洞模板进行自定义、编辑、删除、查询操作
	Web 插件	展示所有的 Web 漏洞类别以及漏洞插件，可以对漏洞模板进行自定义、编辑、删除、查询操作

	口令字典	显示所有的弱口令字典，可以上传自定义口令字典以及删除、查询操作
	基线策略模板	显示所有的基线策略模板，也可以自定义策略模板、编辑、删除、查询操作等
报表管理	数据查询	可查询主机资产和 web 资产的漏洞，也可以通过资产名称、主机、漏洞等来进行筛选查询，以及相关漏洞详情的查看
	对比分析	对不同检测时间段的同一资产进行漏洞对比，以及不同资产组间的漏洞对比
	导出报表	对于扫描完的任务资产可以进行各种类型的报表导出
系统管理	账号管理	修改用户账户的密码
	外发配置	配置邮件、短信、SNMP、SYSLOG、FTP 等相关信息
	告警配置	系统告警日志、配置 CPU、内存等相关的告警信息
	日期/时间	手动设置时间
	漏洞检测备份	任务列表漏洞检测结果备份
	版本/特征库升级	进行特征库在线升级
	诊断工具	对扫描目标可进行 ping 测试以及 wget 测试

	验证工具	进行通用验证和 SQL 注入验证

3. 任务中心

任务中心为用户提供描任务扫描配置、任务下发、任务检测进度、任务检测结果的功能。

3.1.新建任务

新建任务模块主要是针对系统扫描、Web 扫描、口令猜解、仅做存活探测下发相应的扫描任务，分为基础配置和高级选项两大功能。

3.1.1. 基本配置

WEBUI：主界面 -> 任务中心 -> 新建任务 -> 基本配置

基本配置页面是系统扫描，web 扫描，口令猜解，仅做基础探测任务下发的统一入口，提供基础的扫描任务下发配置功能。

图 3.1.1-1 基本配置

基本配置参数说明如表 4.1.1 所示：

表 3.1.1-1 配置参数说明

参数	说明
新建任务类型	包括四种扫描类型：系统扫描，web扫描，口令猜解，仅做基础探测，如勾选仅做基础探测，则不进行漏洞扫描，仅探测资产存活状态和端口开放情况
扫描目标方式	手动输入：针对系统扫描，web扫描，口令猜解，仅做基础探测4中任务，扫描目标填写规范：IP，IP段，域名或者URL
	使用资产：针对系统扫描，web扫描，口令猜解，仅做基础探测4中任务，扫描已生成的资产
	批量导入：针对系统扫描，web扫描，口令猜解，仅做基础探测4中任务，以Excel的格式导入，减少工作量
	会话录制：仅针对WEB扫描，需要在会话录制页面提前录制好会话
扫描目标	被扫描对象，可以是IP，IP段，域名或者URL，多个之间以英文逗号(,)或换行分隔： A.IP示例： 192.168.1.100,2001:fecd:ba23:cd1f:dcb1:1010:9234:4088 B.IP段示例：192.168.1.0/24,192.168.2.1-254,192.168.3.1-192.168.3.254,192.168.1.*

	C.域名示例：www.example.com D.URL示例： http://192.168.1.100/,https://www.example.com/,http://[2001:fecd:ba23:cd1f:dcb1:1010:9234:4088]/ E.排除某个IP：192.168.1.0/24!192.168.1.100
资产组名称	可自定义，默认为默认资产组，也可提前在资产管理界面配置资产组自定义选择
任务名称	可自定义，默认填充为扫描目标
执行方式	支持立即执行、定时执行和周期执行
漏洞插件模板	系统漏洞模板：仅选择系统扫描时展示，默认23种，可自定义，一般建议使用全部漏洞扫描模板
	WEB漏洞插件模板：仅选择web扫描时展示，默认10种，可自定义，一般建议使用全部漏洞扫描模板
	口令猜解服务：仅选择口令猜解时展示，默认10种，选择口令猜解默认需要猜解服务类型。如需选择字典，请前往 -> 高级选项-> 口令猜解高级选项配置
	无：选择仅做存活探测的时候，没有展示

分布式引擎	系统将根据引擎的负载情况，智能选择工作引擎，local：系统将会选择本地引擎
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
告警模板	是否需要扫描结束后向指定邮箱，手机用户，微信用户发送扫描结果，需提前在系统管理界面配置模板

3.1.2. 高级选项

高级选项模块为系统扫描，web 扫描，口令猜解，仅做基础探测任务提供多元化的个性配置功能。

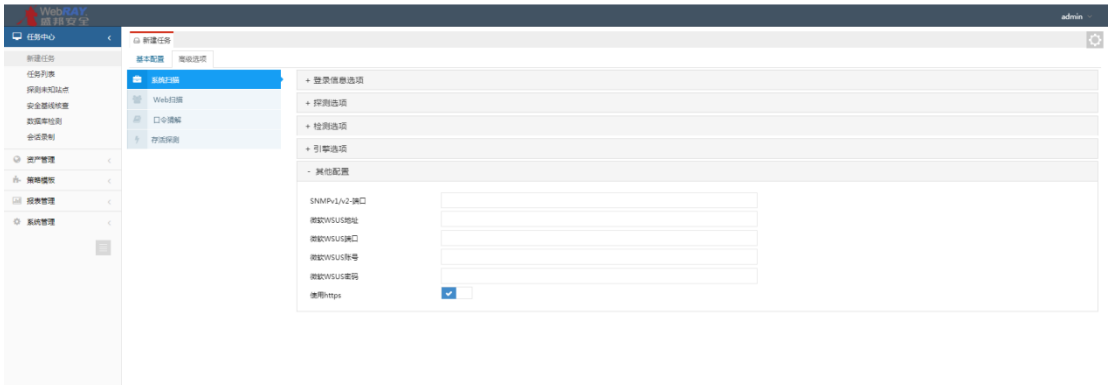


图 3.1.2-1 高级选项

3.1.2.1. 系统扫描--登录信息选项

针对系统扫描，在提交系统扫描任务之前可对扫描目标进行登录验证，可单条添加，也可批量导入。如下图：

图 3.1.2.1-1 系统扫描-登录验证

登录验证配置参数说明如表 3.1.2.1-1 所示：

表 3.1.2.1-1 配置参数说明

参数	说明
目标地址	可填入IP：192.168.1.100 或者域名：www.example.com
服务	目前支持8种服务，SSH、SMB、TELNET、POP、POP3、IMAP、FTP、RDP
端口	登录端口号，整数，[1-65535]之间
用户名	主机登录的用户名
密码	主机登录的密码

3.1.2.2. 系统扫描--探测选项

针对系统扫描，对扫描主机探测的配置功能。

图 3.1.2.2-1 系统扫描-探测选项

探测选项配置参数说明如表 4.1.2.2-1 所示：

表 4.1.2.2-1 配置参数说明

参数	说明
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、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,指定 UDP 端口：UDP:1025-65535
端口扫描方式	可以复选CONNECT或者SYN（但不能全不选） 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TCP SYN包即可完成检测，速度快，建议使用SYN

3.1.2.3. 系统扫描--检测选项

针对系统，高级配置扫描任务的个性化扫描需求。

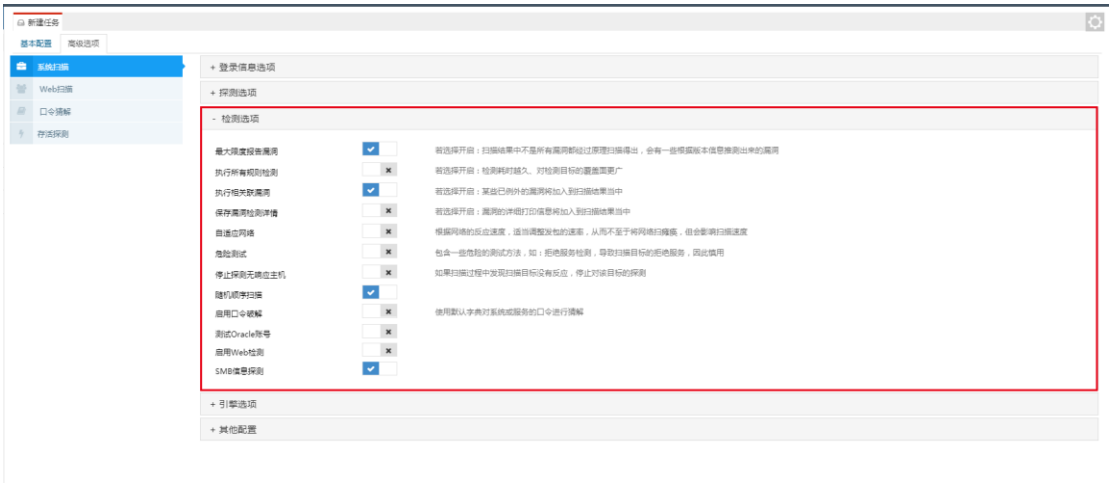


图 3.1.2.3-1 系统扫描-检测选项

检测选项配置参数说明如表 3.1.2.3-1 所示

表 3.1.2.3-1 配置参数说明

参数	说明
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	开启可进行Web检测，如不开启，则不执行WEB安全相关插件
SMB信息探测	启用则可进行SMB信息检测

3.1.2.4. 系统扫描--引擎选项

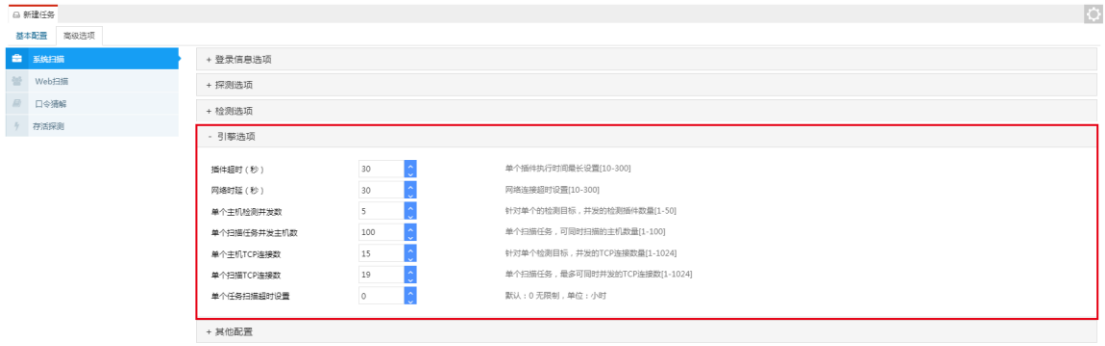


图 3.1.2.4-1 系统扫描-引擎选项

引擎选项配置参数说明如表 3.1.2.4-1 所示：

表 3.1.2.4-1 配置参数说明

参数	说明

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
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]
单个任务扫描超时设置	任务扫描的超时时间，默认：0 无限制，单位：小时

3.1.2.5. 系统扫描--其他配置

图 3.1.2.5-1 系统扫描-其他配置

3.1.2.6. WEB 扫描--登录扫描

针对 WEB 扫描任务，可对扫描任务进行登录配置

图 3.1.2.6-1 Web 扫描-登陆扫描

3.1.2.7. WEB 扫描--引擎配置

图 3.1.2.7-1 Web 扫描-引擎配置

Web 扫描-引擎配置配置参数说明如表 3.1.2.7-1 所示：

表 3.1.2.7-1 配置参数说明

参数	说明
并发线程数	单个扫描目标，并发执行的线程数量[1-50]
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

3.1.2.8. WEB 扫描--检测选项

图 3.1.2.8-1 Web 扫描-检测选项

Web 扫描-检测选项配置参数说明如表 3.1.2.8-1 所示：

表 3.1.2.8-1 配置参数说明

参数	说明
暗链检测	发现网站中的存在的其他隐藏链接
网站木马检测	检测网站中是否存在恶意脚本
检测深度	检测网站中是否存在恶意脚本

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
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，则放弃爬取
例外URL	引擎爬虫不爬取的url关键字，一般为登陆页面、危险操作、或不想做检测的链接等
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

3.1.2.9. 口令猜解--字典选择

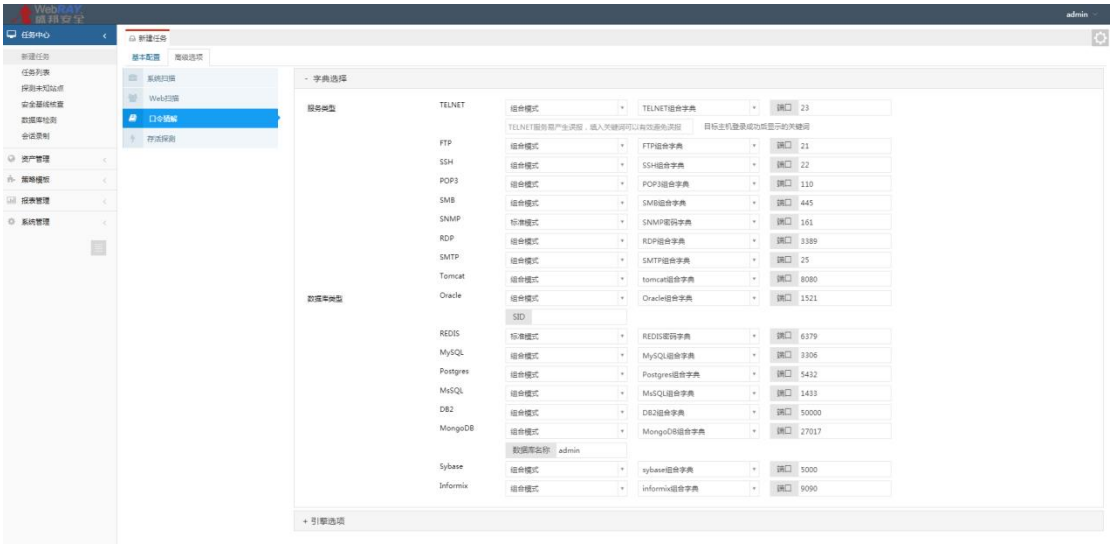


图 3.1.2.9-1 口令猜解--字典选择

字典选择配置参数说明如表 3.1.2.9-1 所示：

表 3.1.2.9-1 配置参数说明

参数	说明
服务类型	支持多种服务类型，字典可选用户名密码组合字典和标准字典，分别是“与”匹配和“或”匹配
数据库类型	支持多种数据库类型，字典可选用户名密码组合字典和标准字典，分别是“与”匹配和“或”匹配

3.1.2.10. 口令猜解-引擎选项

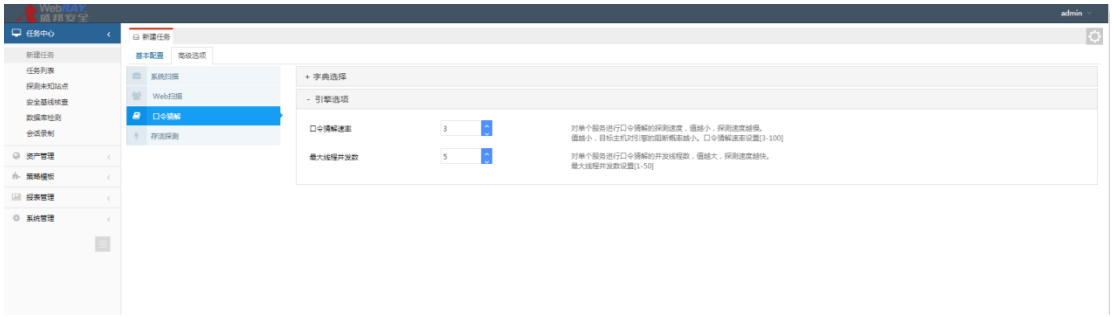


图 3.1.2.10-1 口令猜--引擎选项

口令猜解—引擎选项配置参数说明如表 3.1.2.10-1 所示：

表 3.1.2.10-1 配置参数说明

参数	说明
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

3.1.2.11. 存活探测--探测选项

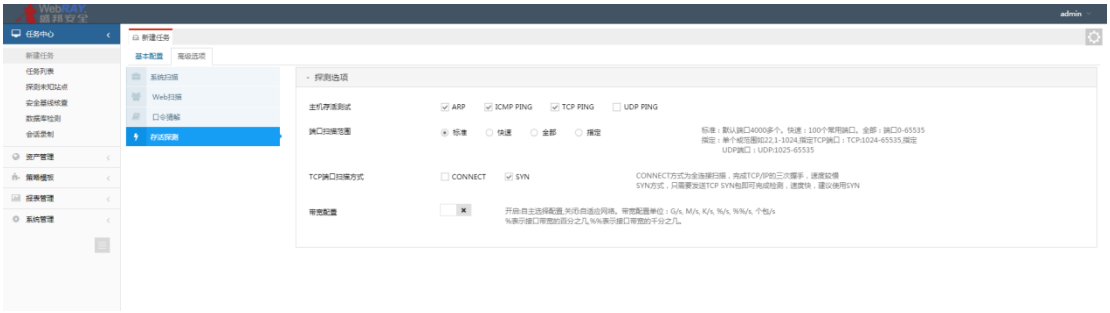


图 3.1.2.11-1 存活探测--探测选项

存活探测--探测选项配置参数说明如表 3.1.2.11-1 所示：

表 3.1.2.11-1 配置参数说明

参数	说明
主机存活测试	对扫描主机的探测方式：ARP,ICMP PING,TCP PING,UDP PING
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
TCP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TCP SYN包即可完成检测，速度快，建议使用

	SYN
带宽配置	开启:自主选择配置,关闭:自适应网络。带宽配置单位：G/s, M/s, K/s, %/s, %%/s, 个包/s，%表示接口带宽的百分之几,%%表示接口带宽的千分之几。

3.2. 任务列表

WEBUI：主界面 -> 任务中心 -> 任务列表->任务列表

3.2.1. 任务列表

任务列表模块主要展示全部的扫描任务，并可对扫描任务进行排序、查看、编辑、删除、以及按任务名称搜索等操作，也可实时且直观的查看任务扫描进度情况，以及对任务的执行操作，如立即执行、禁用等。如图 4.2.1-1 所示

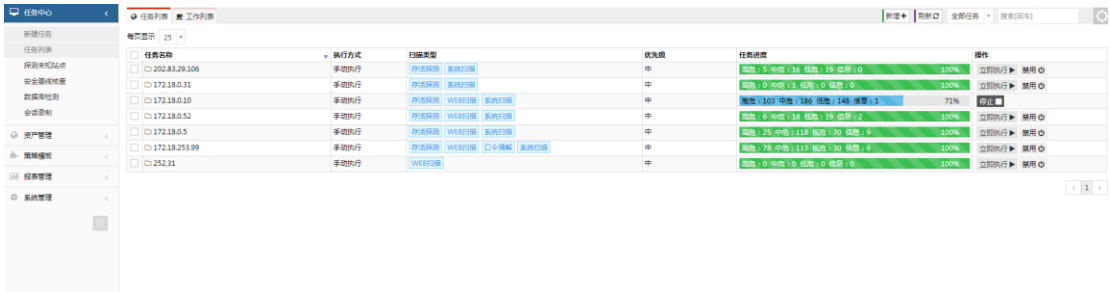


图 3.2.1-1 任务列表总览

任务列表总览配置参数说明如表 3.2.1-1 所示：

表 3.2.1-1 配置参数说明

参数	说明

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
扫描类型	显示当前任务的属于那种扫描任务，包含存活探测，WEB 扫描，口令猜解，系统扫描，数据库扫描
优先级	显示当前任务的优先级，有高中低三种
进度	显示当前任务执行的进度情况，可以查看当前任务的高危，中危，低危，信息漏洞数，仅存活探测任务可以查看探测的系统资产数量和WEB资产数量
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

3.2.1.1. 进度条详情

进度条：任务列表中的进度条会随着扫描时间而实时改变，扫描任务正在进行时会显示发现的相应的漏洞数、资产数等信息

进度条具体详情表如下表所示：

颜色	扫描进度
红色	扫描进度为0%-25%
黄色	扫描进度为25%-50%

蓝色	扫描进度为50%-75%
绿色	扫描进度为75%-100%

任务扫描过程中可以对任务进行暂停、停止等操作，也可以对任务进行继续执行操作，如图所示：

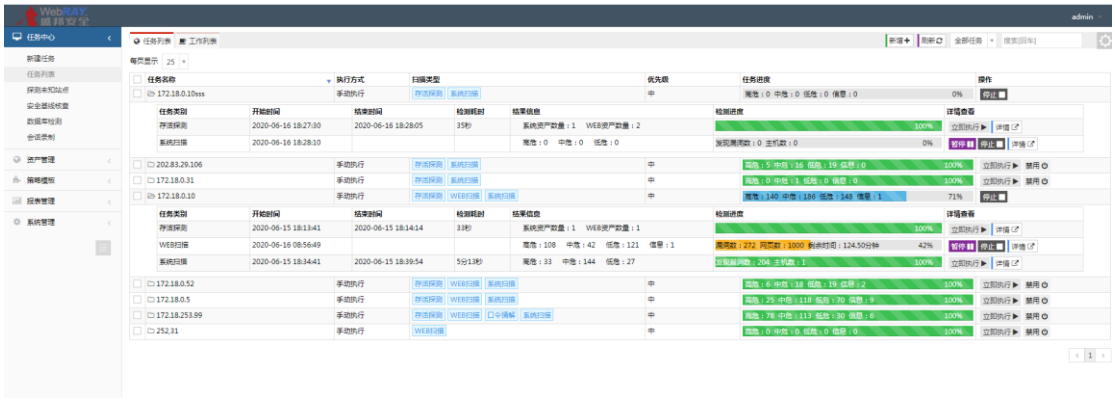


图 3.2.1.1-1 扫描任务执行状态

3.2.1.2. 扫描漏洞详情

系统扫描任务可展示：主机列表、漏洞列表、端口列表以及历史执行记录。点击漏洞列表可查看具体的漏洞详细信息，如图 3.2.1.2-1 所示：

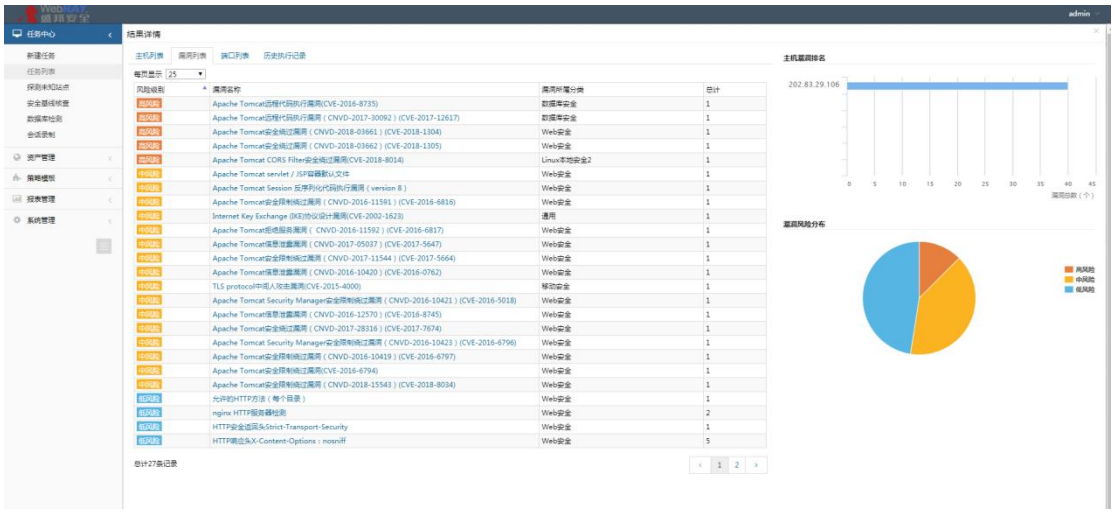


图 3.2.1.2-1 系统扫描漏洞详情

Web 扫描任务可显示：主机列表、漏洞列表、漏洞目录树以及历史执行记

录。点击网站目录结构，可查看漏洞目录树以及对应的漏洞详情，如图 3.2.1.2-2 所示：

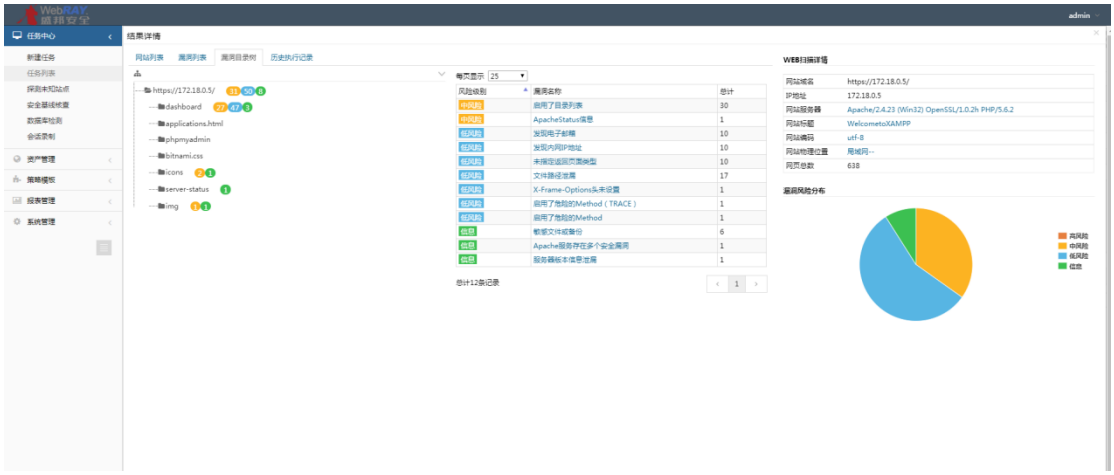


图 3.2.1.2-2 Web 扫描漏洞详情

口令猜解任务可显示：主机列表、弱口令列表以及历史执行记录，如图 3.2.1.2-3 所示：

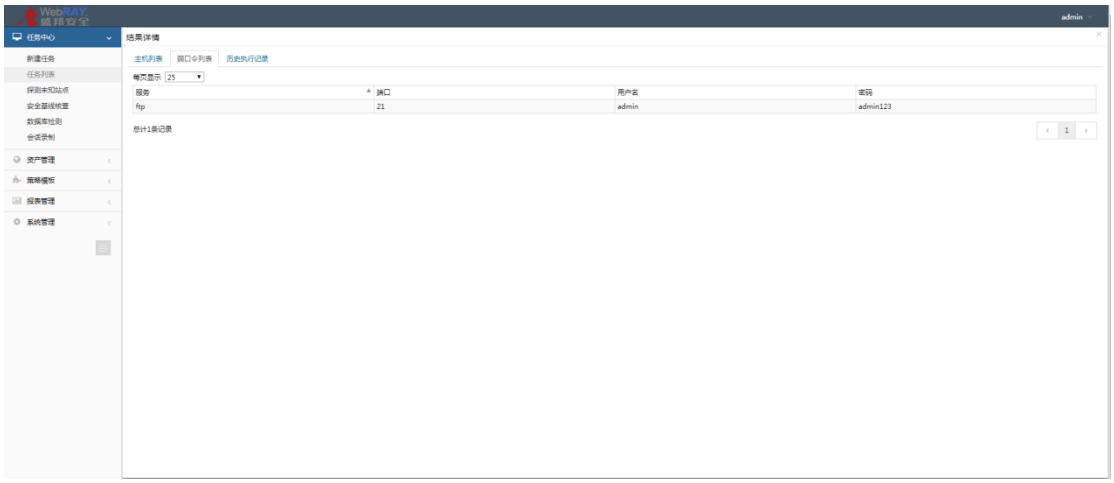


图 3.2.1.2-3 弱口令列表

仅存活探测任务可显示：主机列表、以及历史执行记录，如图 3.2.1.2-4 所示

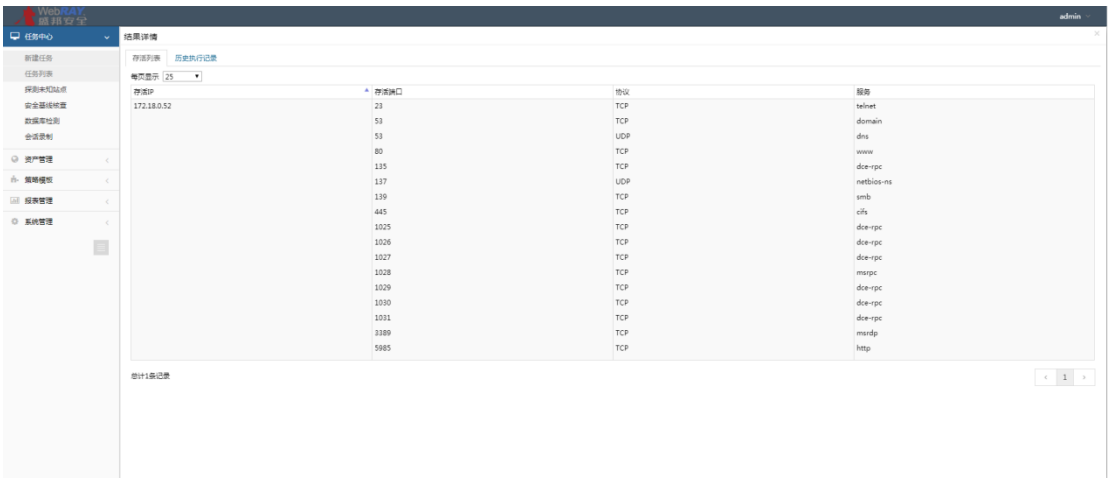


图 3.2.1.2-4 存活列表

3.2.1.3. 任务状态控制

- **立即执行**

在任务列表点击操作栏的【立即执行】，将已完成或者尚未执行的任务立即启动执行

- **禁用**

在任务列表点击操作栏的【禁用】，周期任务将不随周期执行，点击【启用】后，周期任务可正常跟随周期执行

- **停止**

在任务列表点击操作栏的【停止】，将正在执行的任务全部停止，任务不再执行，点击立即执行后，任务会重新下发进行执行

- **暂停**

在任务列表点击操作栏的【暂停】，将正在执行的任务暂停，点击【继续】，暂停的任务会接着暂停前的进度继续执行，不会重新下发

图 3.2.1.3-1 任务暂停

3.2.1.4. 编辑任务

操作：（1）在任务列表页面，选择任务->点击【编辑】，跳转到任务配置页面，对任务配置进行修改，资产组名称和扫描目标不支持编辑， 如下

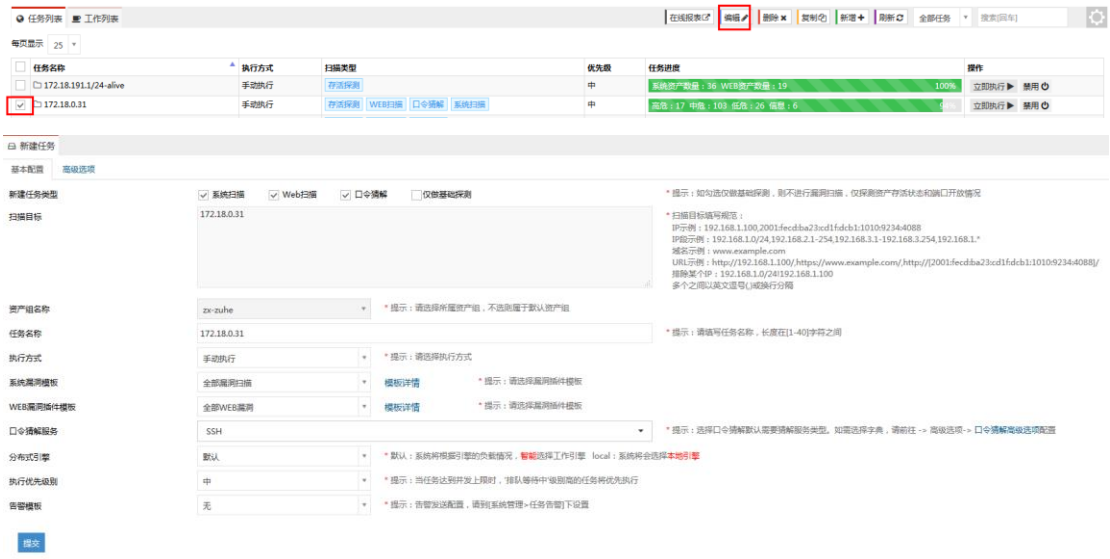


图 3.2.1.4-1 编辑任务

（2）修改任务配置后点击【提交】，任务重新执行时会按照修改后的配置进行扫描

3.2.1.5. 删除任务

操作：（1）在任务列表页面，选择任务->点击【删除】->确认，即可将所选任务删除，任务删除后，任务生成的资产不会被删除，但是该资产就无法导出报表

图 3.2.1.5-1 删除任务

3.2.1.6. 复制任务

复制任务是复制任务的配置信息，需输入扫描目标和任务名称

操作：（1）在任务列表页面，选择任务->点击【复制】->弹窗显示复制任务的输入框，如下

图 3.2.1.6-1 复制任务目标输入

（2）输入扫描目标和任务名称后点击【提交】，即可在任务列表生成任务

图 3.2.1.6-2 复制任务

3.2.1.7. 查看任务在线报表

只有经过系统扫描、web 扫描或者口令猜解的任务可查看在线报表，若任务尚未执行或者任务类型是仅存活探测任务，则无法查看在线报表

操作：（1）在任务列表页面，选择任务->点击【在线报表】，直接自动新建标签页进入任务的统计报表页面，即可查看该任务的统计报表，如下

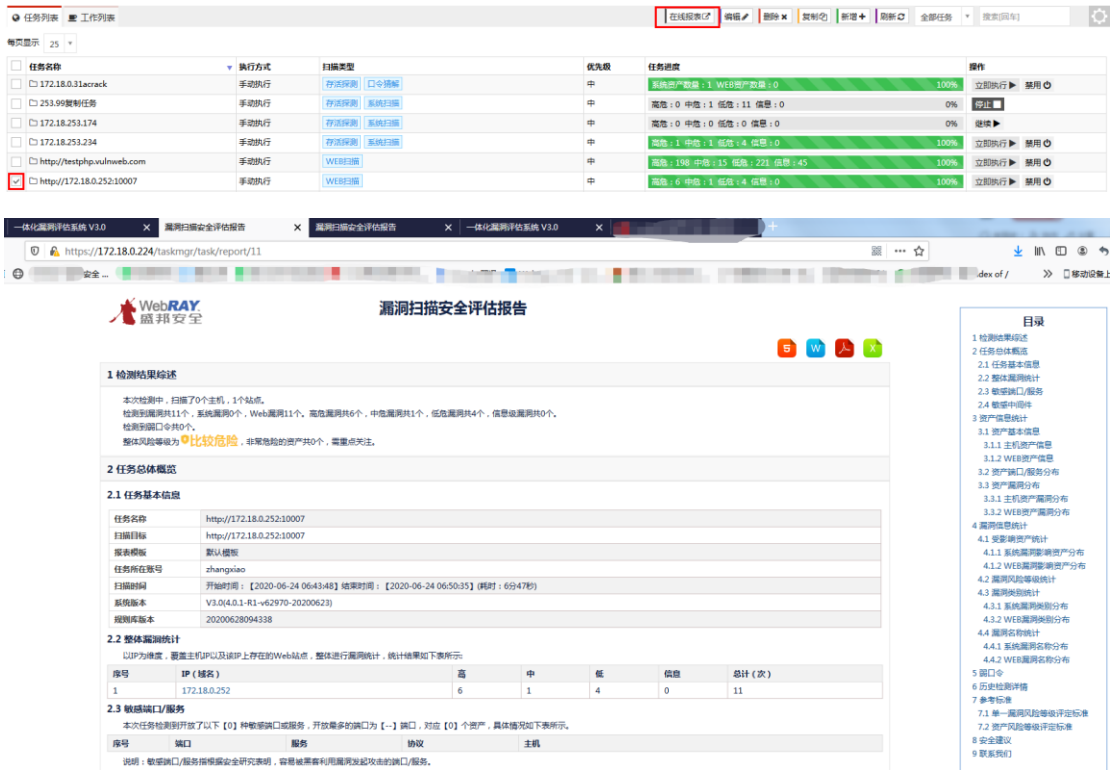


图 3.2.1.7-1 在线报表-统计报表

（2）点击统计报表里【2.2 整体漏洞统计】章节的 IP（域名），直接新开标签页跳转到所点击资产的详细报表页面，即可查看所点击资产的详细报表

漏洞扫描安全评估报告

1 检测结果综述

本次报告中，目标【172.18.0.252】共检测出风险11个，其中系统漏洞0个，Web漏洞11个，弱口令0个。

整体风险值为6.6，安全等级为比较危险。所有漏洞中，高危漏洞6个，中危漏洞1个，低危漏洞4个，信息级漏洞0个。（漏洞风险等级的分类规则及资产风险等级分类规则，请参见章节《资产风险等级评定标准》）。

2 资产总体概览

2.1 资产基本信息

系统资产列表：

WEB资产列表：

Web资产	http://172.18.0.252:10007/
网站域名	172.18.0.252
IP地址	172.18.0.252
服务器信息	
网站标题	S2-053Demo
网站编码	UTF-8
服务器语言	
网站物理地址	
扫描时间	开始时间：【2020-06-24 06:43:48】结束时间：【2020-06-24 06:50:35】(耗时：6分47秒)
资产风险值	6.6
漏洞分布	漏洞总计：11 高风险：6 中风险：1 低风险：4 信息：0
漏洞状态标识	新增：11 误报：0 已修复：0
资产组	zx-webscan

图 3.2.1.7-2 在线报表-详细报表

- **在线报表导出到本地**

操作：点击在线报表右上方的  ，即可将任务报表导出到本地

3.2.2. 工作列表

WEBUI：主界面 -> 任务中心 -> 任务列表->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停止或强制停止操作，也可以对工作列表进行排序、搜索等。具体界面如图 3.2.2-1 所示：

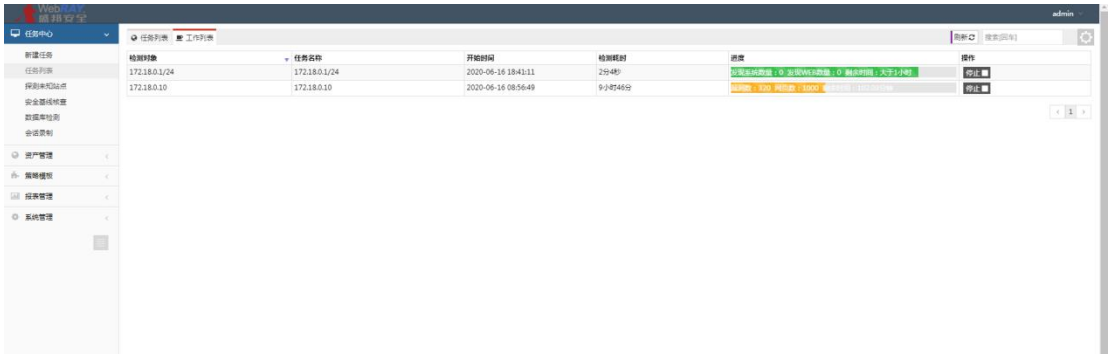


图 3.2.2-1 工作列表

工作列表各项参数说明如表 3.2.1-1 所示：

表 3.2.1-1 各项参数说明

参数	说明
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

⚠注意： 工作列表中的进度条显示的是单个任务的单个检测目标，一个任务可包含多个扫描目标，相应的也会有多个工作列表。

3.3.探测未知站点

WEBUI：主界面 -> 任务中心 -> 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。可对探测到的未知站点进行编辑、删除等操作，也可新建探测未知站点。探测未知站点列表详情如图 3.3 所示：

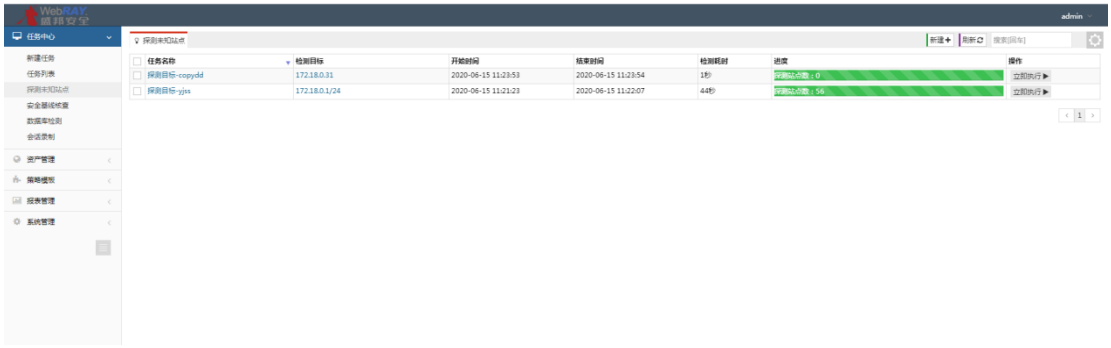


图 3.3 探测未知站点列表

3.3.1. 新建探测任务

点击【新建】按钮，在弹出的页面中填写任务名称、探测 IP 范围以及探测端口相关信息，点击【开始探测】按钮即可新建探测任务成功，具体详情如下图 3.3.1 所示：

图 3.3.1 新建探测任务

新建探测任务配置参数说明如表 3.3.1 所示：

表 3.3.1 配置参数说明

参数	说明
探测IP/IP范围	填写扫描扫描IP，多个之间以英文逗号(,)或换行分隔
探测端口范围	填写web站点常用的端口及自定义端口，多个之间以英文逗号(,)分隔

3.3.2. 探测详情

点击任务名称、检测目标或进度条即可跳转至未知站点的探测详情，如下图 3.3.2 所示：

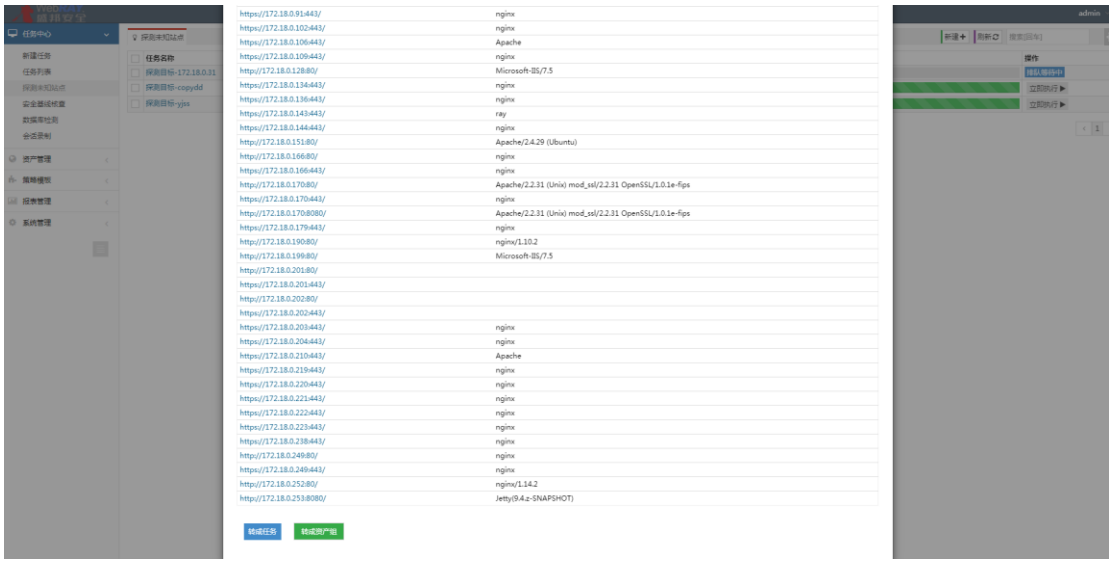


图 3.3.2 探测详情

探测详情配置参数说明如表 3.3.2 所示：

表 3.3.2 配置参数说明

参数	说明
转成任务	自动跳转到新建任务，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，用户可选择自定义的资产组

3.4.安全基线核查

安全基线扫描可针对基线核查任务进行编辑、删除、排序等，可以根据列表显示查看到任务名称、扫描策略、开始时间、结束时间和扫描进度；启动按钮可以重新复制任务扫描基线;在线报表可以查看基线扫描结果详情。具体如下图 3.4 所示:

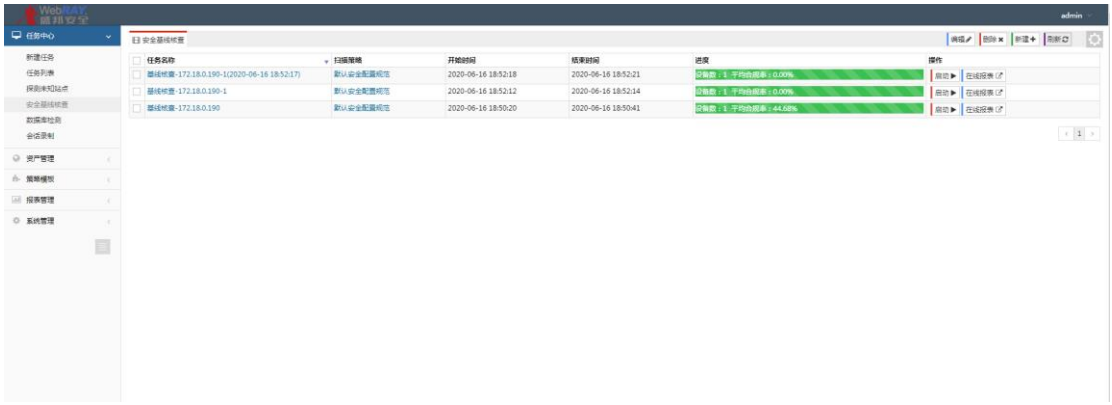


图 3.4 基线核查任务列表

3.4.1. 新建基线核查任务

基线任务列表右上角点击【新建】按钮，可以新建基线核查任务，登录用户名以及密码，可点击【登录验证】，若验证成功，则会提示“登录目标主机成功”。填写相应的任务名称、扫描策略、检测模板后，点击立即执行按钮，即可新建任

务成功。如图 3.4.1 所示：

图 3.4.1 新建基线核查任务

新建基线核查任务配置参数说明如表 3.4.1 所示：

表 3.4.1 配置参数说明

参数	说明
检测目标方式	手动输入和批量导入两种，批量导入需下载相应的模板进行导入
检测目标	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：192.168.1.10 主机组示例：192.168.1.1-192.168.1.10 范围不超过 255 个
登录协议	选择基线扫描目标开放的协议
协议端口	根据选择的登录协议，自动匹配显示协议的默认端口。 如果协议自定义端口，需手动修改。

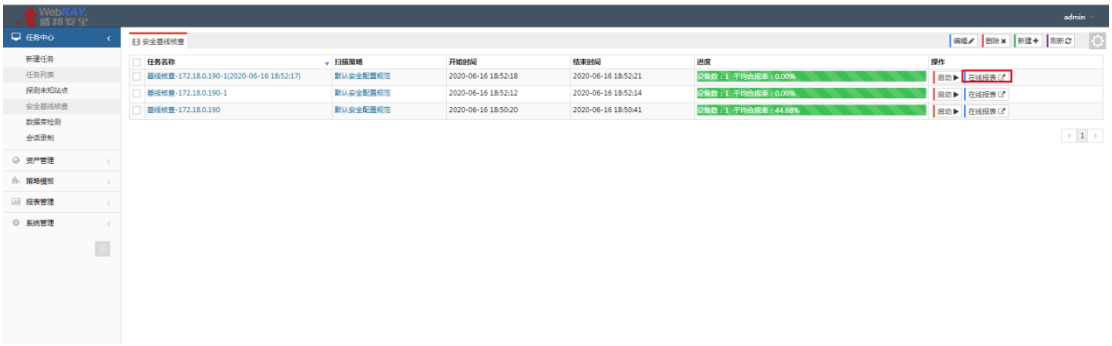
	示例:ssh 协议　22 端口(默认端口)
登陆账号	输入目标主机的相关账号 示例:Administrator(Windows 主机);root(Linux 主机).
登陆密码	输入相关账号对应的密码
任务名称	输入基线扫描任务的任务名称
扫描策略	根据客户自己行业性质、单位要求标准等选择所需的扫描策略
检测模板	根据检测目标主机的情况，选择相应的扫描模板
数据库配置模板(模板高级选项)	根据所选的检测模板，自动列出对应数据库配置模板. 输入数据库配置模板相对应的配置. 示例:mysql 数据配置 /usr/bin/mysql
应用服务器模板(模板高级选项)	根据所选的检测模板，自动列出对应应用服务器配置模板. 输入应用服务器配置模板相对应的配置. 示例: WebSphere 配置 /opt/IBM/WebSphere/AppServer_1/
登陆验证	测试对应协议登陆主机用户名及密码是否正正确，协议所选是否支持

3.4.2. 基线任务在线报表

基线任务列表操作列点击【在线报表】按钮，即可查看相应的报表，同时在线报表也支持下载到本地。

基线扫描报表分为安全配置核查综合评估报告和设备安全配置合规分析报告两部分。

安全配置核查综合评估报告点击主机或点击数据库或应用服务器，可查看对应设备安全配置合规分析报告。



3.4.2.1. 安全配置核查综合评估报告

评估报告导出报表格式为 HTML,Excel,XML 格式。

安全配置核查综合评估报告分为概览、核查结果汇总、核查失败设备列表和不合规检查项汇总四部分。

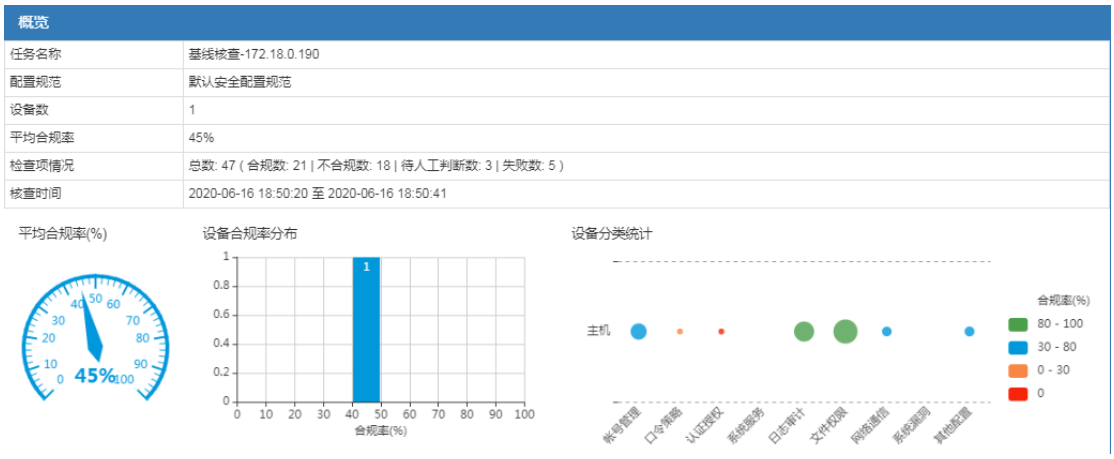


图 3.4.2.1-1 评估报表概览

核查结果汇总

类型/设备名称	设备IP	配置模板	合规率	检查项				
				总数	合规数	不合规数	人工判断数	失败数
安全设备 (1)								
防火墙 (1)								
172.18.0.72	172.18.0.72	天融信防火墙配置模板	18%	22	4	17	1	0

图 3.4.2.1-2 评估报表核查结果汇总

不合规检查项汇总

类型/检查项编码	检查项名称	严重级别	不合规设备数
安全设备 (17)			
防火墙 (17)			
Topsec(FW)-4	口令长度和复杂度	高危	1
Topsec(FW)-3	口令加密	高危	1
Topsec(FW)-13	远程通信管理安全	高危	1
Topsec(FW)-8	记录用户登录日志	中危	1
Topsec(FW)-7	授权粒度控制	中危	1
Topsec(FW)-5	账户锁定策略	中危	1
Topsec(FW)-17	配置日志存储位置	中危	1
Topsec(FW)-12	远程主机IP地址段限制	中危	1
Topsec(FW)-9	记录用户操作行为日志	中危	1
Topsec(FW)-22	路由协议认证	中危	1
Topsec(FW)-6	web管理应该开启图形验证码功能	低危	1
Topsec(FW)-1	避免共享账号	低危	1
Topsec(FW)-10	日志加密	低危	1
Topsec(FW)-18	启用NTP服务	信息	1
Topsec(FW)-19	隐藏banner信息	信息	1
Topsec(FW)-21	防止仿冒ARP网关攻击	信息	1
Topsec(FW)-11	会话超时配置	信息	1

图 3.4.2.1-3 评估报表不合规检查汇总

3.4.2.2. 设备安全配置合规分析报告

设备安全配置合规分析报告分为设备概览、相关配置模板信息和设备扩展信息三部分内容。

设备概览

设备名称	172.18.0.190
核查模板	Redhat/CentOS 6.x配置模板
设备IP	172.18.0.190
合规率	45%
检查项情况	总数: 47 (合规数: 21 | 不合规数: 18 | 待人工判断数: 3 | 失败数: 5)
核查时间	2020/06/16 18:50:18
核查任务	基线核查-172.18.0.190

图 3.4.2.2-1 分析报告设备概览

点击设备概览的核查任务，可查看相对应的安全配置核查综合评估报告。

Redhat/CentOS 6.x配置模板

分类/编号	名称	严重级别	结果	详情
帐号管理 (3)				
Linux-6	检查是否设置除root之外UID为0的用户	中危	合规	
Linux-27	检查是否按用户分配账号	中危	合规	
Linux-30	检查是否删除与设备运行、维护等工作无关的账号	信息	人工判断	
口令策略 (7)				
Linux-1	检查是否设置口令生存周期	高危	不合规	
Linux-2	检查是否设置口令更改最小间隔天数	高危	不合规	
Linux-3	检查设备密码复杂度策略	高危	不合规	
Linux-4	检查是否设置口令过期前警告天数	高危	合规	
Linux-5	检查是否存在空口令账号	高危	检查失败	
Linux-23	检查密码重复使用次数限制	中危	不合规	
Linux-46	检查账户认证失败次数限制	中危	不合规	
认证授权 (2)				
Linux-7	检查用户目录缺省访问权限设置	高危	不合规	
Linux-8	检查是否设置SSH登录前警告Banner	中危	检查失败	
日志审计 (6)				
Linux-9	检查是否对登录进行日志记录	高危	合规	
Linux-10	检查是否启用cron行为日志功能	信息	合规	
Linux-11	检查是否配置远程日志功能	信息	不合规	
Linux-12	检查是否配置su命令使用情况记录	信息	合规	
Linux-25	检查日志文件权限设置	中危	合规	
Linux-42	检查安全事件日志配置	信息	合规	
文件权限 (2)				
Linux-26	检查FTP用户上传的文件所具有的权限	中危	合规	
Linux-47	检查重要目录或文件权限设置	中危	合规	

图 3.4.2.2-2 分析报告 Redhat/Centos6x 模板

点击人工判断图标，可查看具体详情。如下图 3.4.2.2-3：

Linux-30 检查是否删除与设备运行、维护等工作无关的账号 信息 人工判断

理论依据

配置要求：
应删除或锁定与设备运行、维护等工作无关的账号。

审计步骤

检查步骤：
执行如下命令查看系统未锁定的账号：

```
#cat /etc/shadow|sed '/^\s*#/d'|awk -F: '($2!~/^*/) && ($2!~/^!!/) {print $1}'
```

合规标准：
人工确认项，用户依据实际情况判断未锁定的账号是否存在与设备运行、维护工作无关的账号。

检查点

⊗ 可用的用户列表 检查失败

加固方案

```
1、删除用户：
#userdel username
2、锁定用户：
#passwd -l username      #锁定用户，只有具备超级用户权限的使用者方可使用。
#passwd -d username      #解锁用户，解锁后原有密码失效，登录设置新密码才能登录。
#passwd -u username      #解锁用户后，原密码仍然有效。
3、修改用户shell域为/bin/false
#usermod -s /bin/false username  #命令来更改相应用户的shell为/bin/false，其中[name]为要修改的具体用户名。
```

图 3.4.2.2-3 分析报告人工判断具体详情

3.5.数据库检查

WEBUI：主界面 -> 任务中心 -> 数据库检查

3.5.1. 检测基本配置

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。具体如下图 3.5.5.1-1 所示：

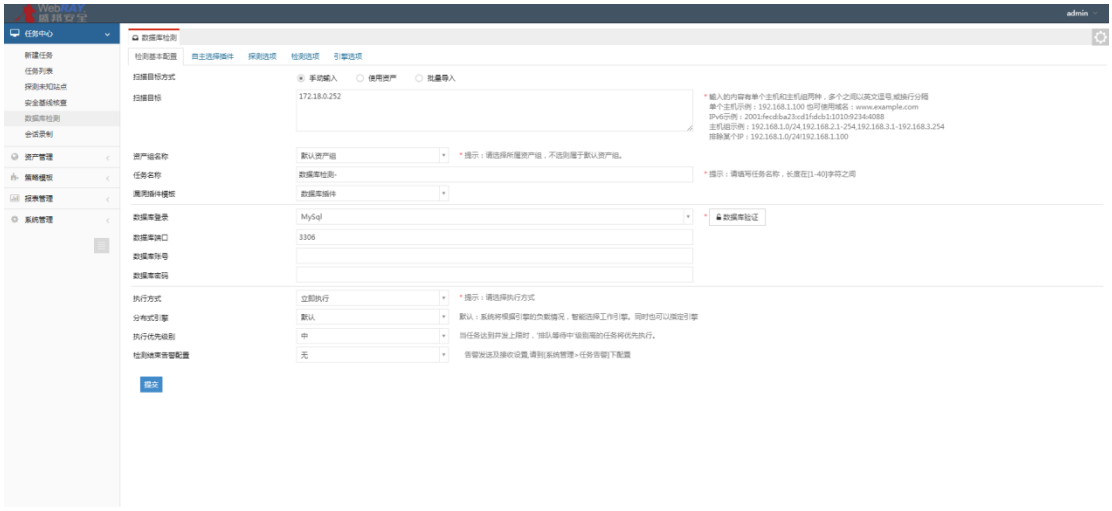


图 3.5.1-1 新建数据库扫描任务

新建数据库扫描任务配置参数说明如表 3.5.1-1 所示：

表 3.5.1-1 配置参数说明

参数	说明
扫描目标方式	手动输入：可输入单个主机或主机组，即扫描对象
	使用资产：扫描已知资产，资产管理界面需要有资产
	批量导入：以Excel的格式导入，减少工作量
扫描目标	被扫描对象，可以是单个主机或主机组

	* 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
资产组名称	可自定义，默认为默认资产组，也可提前在资产管理界面配置资产组自定义选择
任务名称	可自定义，默认前缀是为了区分不同的扫描任务
数据库登录	支持常规数据库检测及其认证方式
执行方式	支持立即执行、定时执行和周期执行
漏洞插件模板	选择数据库漏洞插件模板
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
分布式引擎	是否作为分布式扫描引擎工作，常规扫描‘默认’即可

检测结束告警配置	是否需要扫描结束后向指定邮箱，手机用户，微信用户发送扫描结果，需提前在系统管理界面配置模板

3.5.2. 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。

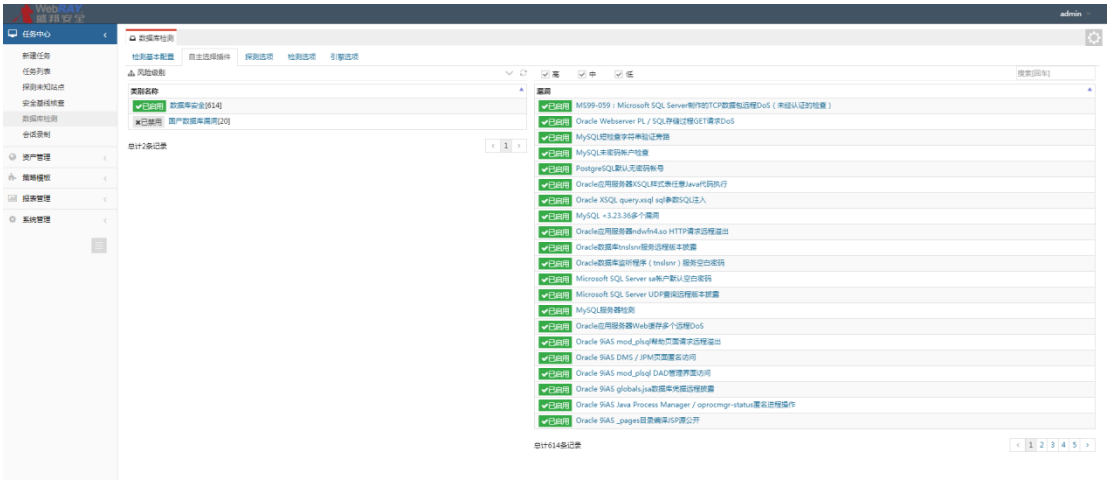


图 3.5.2-1 数据库扫描-自主选择插件

3.5.3. 探测选项

图 3.5.3-1 数据库扫描-探测选项

数据库扫描-探测选项配置参数说明如表 3.5.3-1 所示：

表 3.5.3-1 配置参数说明

参数	说明
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、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,指定UDP端口：UDP:1025-65535
端口扫描方式	可以复选CONNECT或者SYN（但不能全不选） 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TCP SYN包即可完成检测，速度快，建议使用SYN

3.5.4. 检测选项

图 3.5.4-1 数据库扫描-检测选项

数据库扫描-检测选项配置参数说明如表 3.5.1.4-1 所示：

表 3.5.4-1 配置参数说明

参数	说明
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	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

3.5.5. 引擎选项

图 3.5.5-1 数据库扫描-引擎选项

数据库扫描-引擎选项配置参数说明如表 3.5.5-1 所示：

表 3.5.5-1 配置参数说明

参数	说明

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
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]

3.6. 会话录制

WEBUI：主界面 -> 任务中心 ->会话

会话录制功能可以将用户浏览记录保存下来，方便用户批量下发任务

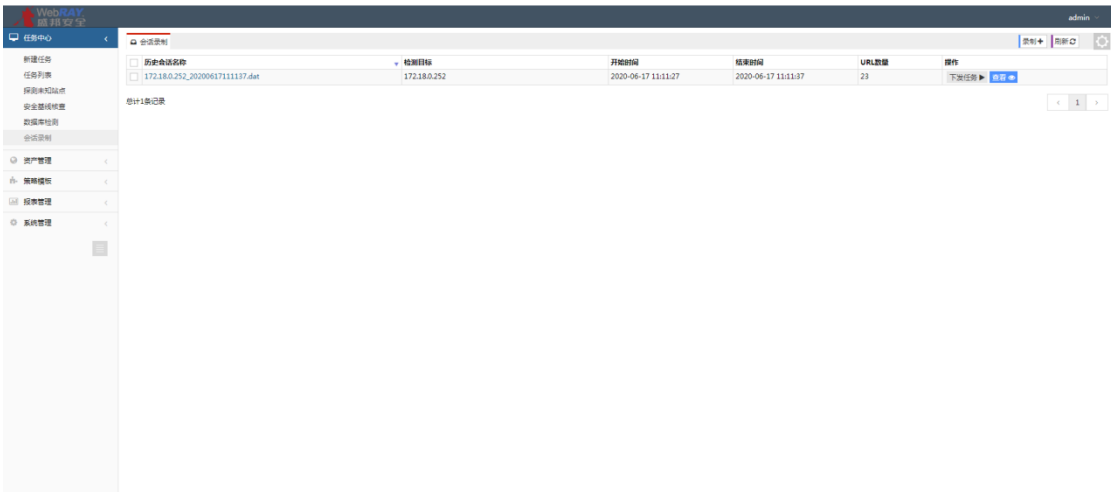


图 3.6-1 会话录制界面

操作：（1）点击录制按钮，按照提示配置录制配置，录制功能界面如下图3.6-2

图 3.6-2 录制界面

（2）录制完成后，点击停止录制

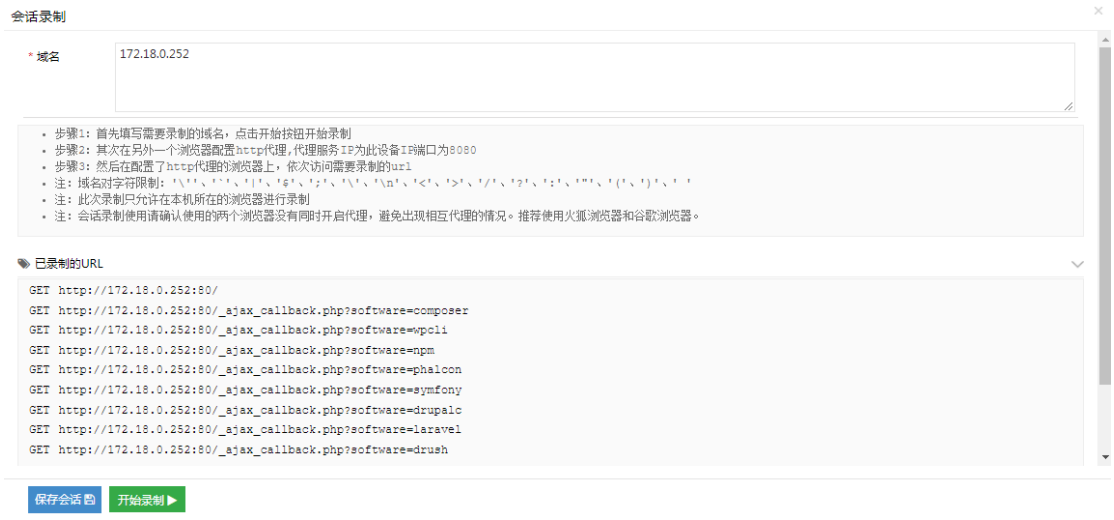


图 3.6-3 录制结束

（3）保存会话：

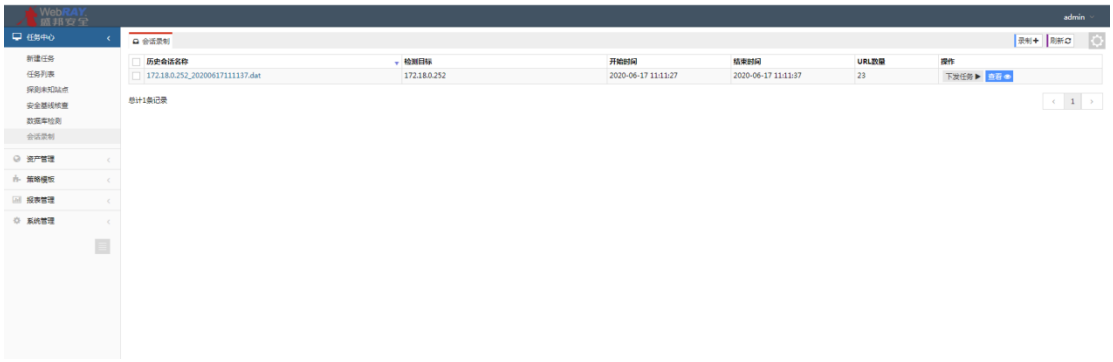


图 3.6-4 保存会话成功

（3）在会话录制列表可查看录制的 url，也可点击【下发任务】，可直接跳转到 web 扫描任务配置页面：

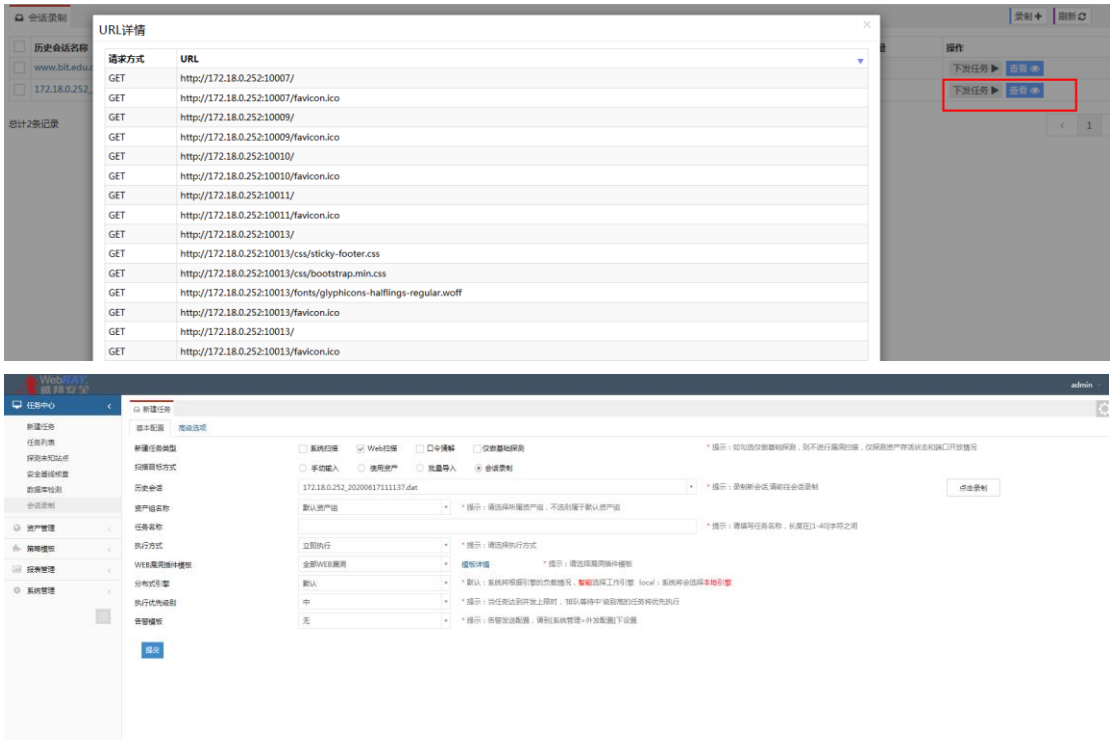


图 3.6-3 采用会话下发扫描任务

4. 资产管理

WEBUI：主界面 -> 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。资产管理界面如图 5 所示：

图 4-1 资产管理

对于其中一个资产，点击可以显示资产树，资产树由资产组、主机节点、主机以及主机上的 web 资产组成，管理员可以通过查看资产树来了解自己的网络资产情况，也可以在搜索框中按照不同维度条件搜索资产。

4.1.资产管理

4.1.1. 主机资产

主机资产：展开资产树中的资产组，选择目标节点展开，节点下的主机资产由历史系统扫描任务、存活任务和用户添加生成，点击主机资产，会显示该资产的资产风险值，漏洞详情、资产属性等。

- **主机漏洞详情**

展示了所选资产最后一次检测时间段的漏洞数，具体到高、中、低危以及信息级漏洞总数，如图 4.1-1 所示：

图 4.1-1 主机资产管理-漏洞详情

操作：点击【漏洞名称】可查看漏洞详情，即漏洞描述、解决办法、扫描详情、漏洞状态等

- **资产属性**

展示了所选资产最后一次扫描的主机信息，包括该资产的主机地址、主机名称、操作系统、物理地址以及主机资产评分等信息，如图 4.1-2 所示：

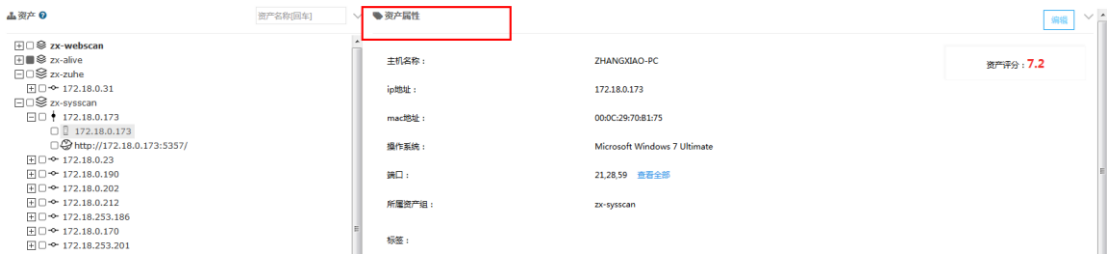


图 4.1-2 系统资产管理-资产指纹信息

操作：点击端口的【查看全部】，可弹窗展示主机上开放的所有端口

操作：点击弱口令的【查看全部】，可弹窗展示主机上检测出的弱口令和密码

4.1.2. Web 资产

Web 资产：展开资产树中的资产组，选择目标节点展开，节点下的 web 资产由历史 web 扫描任务、存活任务和用户添加生成，点击 web 资产，会显示该资产的资产风险值，漏洞详情、资产属性等。

- **Web 资产漏洞详情**

展示了最近一次扫描结果中的所有漏洞相信信息，包括某一漏洞的风险级别、插件名称、插件所属分类以及总数，如图 4.1.2-1 所示：

图 4.1.2-1 Web 资产管理-漏洞详情

操作：点击【漏洞名称】可查看漏洞详情，即漏洞描述、解决办法、扫描详情、漏洞状态等

- **资产属性信息**

展示了每个 web 资产的主机信息，包括该资产的网站域名、IP 地址、服务器信息、网站标题、网站编码、物理地址等指纹信息，如图 4.1.2-2 所示：

图 4.1.2-2 Web 资产管理-资产属性信息

4.1.3. 新增资产

- **手动新增资产**

点击【新增资产】按钮，在弹出的对话框中输入资产目标，选择目标对应的资产组，可自定义是否要添加标签，完成后点击【提交】按钮即可。具体详情如图 4.1.3-1 所示：

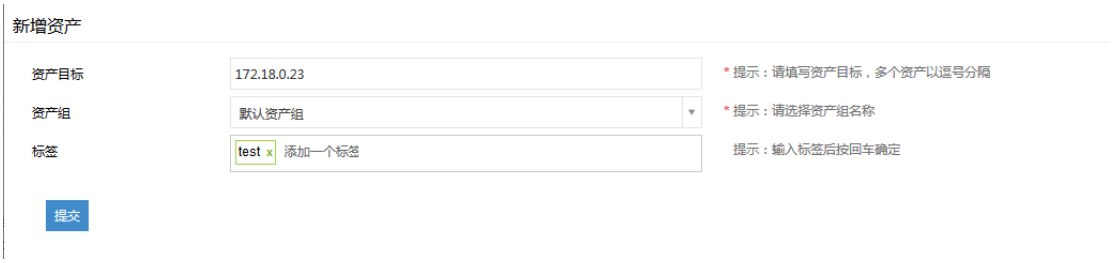


图 4.1.3-1 Web 资产管理-新建资产

备注：资产目标支持单个、多个目标的输入，也支持 ip、url、域名多种目标格式的输入，多个资产逗号分隔

- **批量导入资产**

点击批量导入->下载模板文件->将提前准备好的资产复制到模板文件中->上传文件-》选择所属资产组，自定义是否要添加标签-》上传

图 4.1.3-2 Web 资产管理-新建资产

➢ **资产添加/删除标签**

可选择多个或者单个资产对其添加标签进行分类，添加标签操作如下：

1) 手动新增资产时，直接添加标签->提交即可

2) 历史任务自动生成的资产->点击编辑，添加标签后提交即可

4.1.4. 删除资产

用户可以对资产进行删除，可删除整个资产组、整个节点、也可删除某一节点下的资产。具体详细信息如图 4.1.4-1：

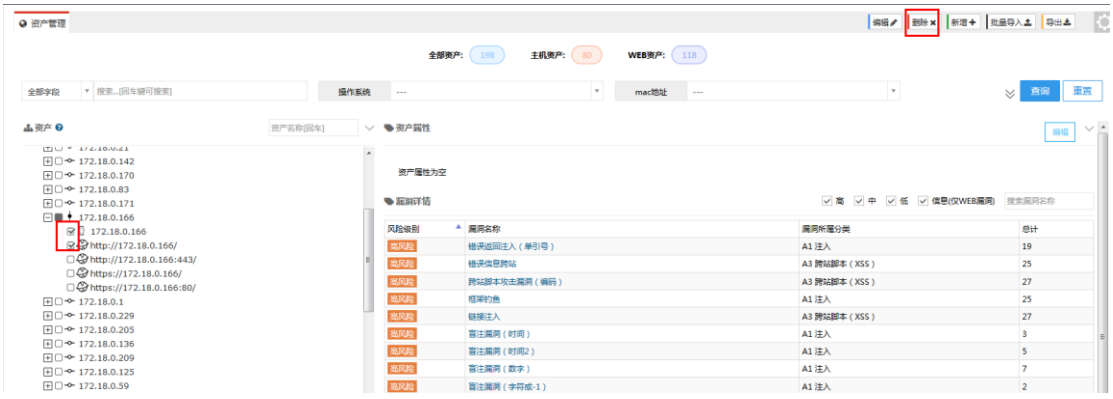


图 4.1.4-1 Web 资产管理-删除资产

4.1.5. 编辑资产

可以选择单个资产编辑所选资产的资产属性，也可选择多个资产、多个节点、多个资产组进行批量编辑，对资产进行分组和添加标签

图 4.1.5-1 编辑资产属性

批量编辑资产组和标签操作如下：

1) 在资产管理界面->选择多个资产、或者多个节点、或者多个资产组->点击【编辑】

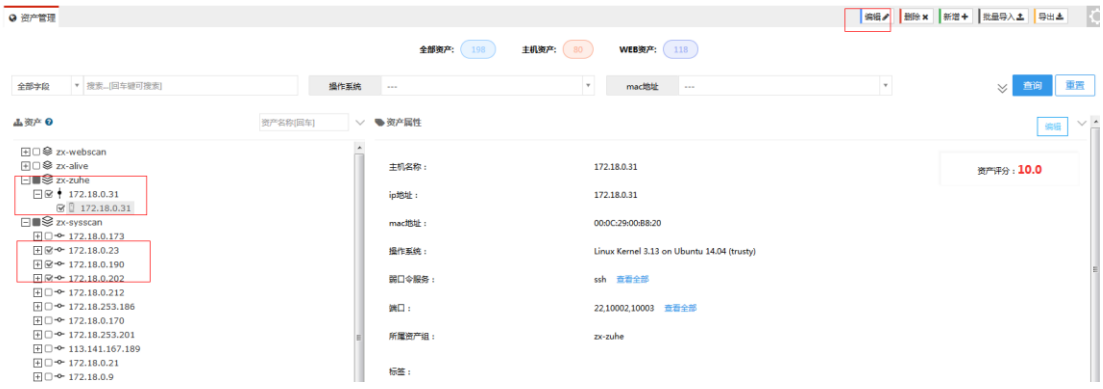


图 4.1.5-2 批量编辑资产属性

2) 修改所属资产组和标签-》点击【提交】，即可成功修改所选资产的所属

资产组和标签

图 4.1.5-3 批量编辑资产属性

4.1.6. 查询资产

支持多个维度的条件搜索，具体搜索操作如下：

1) 进入资产管理界面->点击，展开所有搜索条件，如下

图 4.1.6-1 资产搜索条件

2) 配置不同查询参数->点击查询，查看符合条件的资产信息

图 4.1.6-2 资产搜索

查询条件参数说明：如下表

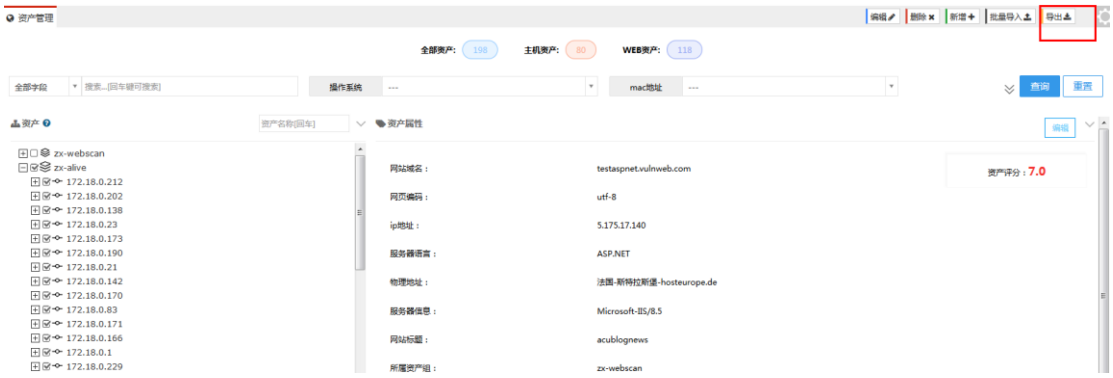
表 4.1.6-1 搜索条件参数说明

参数	描述
资产名称	主机资产或者web资产名称
资产 ip	主机资产的ip
资产 url	Web资产的url
服务器信息	Web资产使用的服务器信息
网页编码	Web资产使用的网页编码技术
服务器语言	Web资产使用的服务器语音
物理地址	资产设备所在的物理地址
操作系统	主机设备的操作系统类型
Mac 地址	主机设备的mac地址
资产组	资产所属的资产组，下发任务时指定或者新增资产时指定
标签	资产标签，由用户定义
评分	资产经过扫描后的系统给出的风险值，风险值越高说明资产越不安全

3） 单击【重置】按钮，可以清空查询条件，重新查询资产信息。

4.1.7. 资产导出

在资产管理界面->选择资产或者不选择->点击导出按钮，如下：可将系统上所选资产或者全部资产导出到 excel



A	B	C	D
资产组名称	主机	资产名称	
默认资产组	172.18.191.81	172.18.191.81	
		http://172.18.191.81:8000/	
	172.18.191.219	172.18.191.219	
	172.18.191.225	172.18.191.225	
		https://172.18.191.225/	
	172.18.191.51	172.18.191.51	
	172.18.191.40	172.18.191.40	
		http://172.18.191.40:1028/	
	172.18.191.96	172.18.191.96	
		http://172.18.191.96:3000/	
		https://172.18.191.96/	
	172.18.191.128	172.18.191.128	
	172.18.191.234	172.18.191.234	
		http://172.18.191.234:1073/	
	172.18.191.102	172.18.191.102	
	172.18.191.1	172.18.191.1	
		http://172.18.191.1:443/	
	172.18.191.58	172.18.191.58	
	172.18.191.22	172.18.191.22	
	172.18.191.89	172.18.191.89	
	172.18.191.163	172.18.191.163	
	172.18.191.143	172.18.191.143	
	172.18.191.32	172.18.191.32	
		https://172.18.191.32/	
	172.18.191.11	172.18.191.11	
	172.18.191.57	172.18.191.57	
		http://172.18.191.57:5357/	
	172.18.191.19	172.18.191.19	
	172.18.191.150	172.18.191.150	
	172.18.191.249	172.18.191.249	
	172.18.191.103	172.18.191.103	
	172.18.191.175	172.18.191.175	
		http://172.18.191.175:5357/	
	172.18.191.154	172.18.191.154	
		http://172.18.191.154:5357/	
		http://172.18.191.154:8082/	
	172.18.191.214	172.18.191.214	

资产

图 4.1.7-1 资产导出

4.2.资产组管理

WEBUI：主界面 -> 资产管理->资产组管理

4.2.1. 新增资产组

操作：在资产组管理页面->点击【新增】->输入资产组名称->点击提交

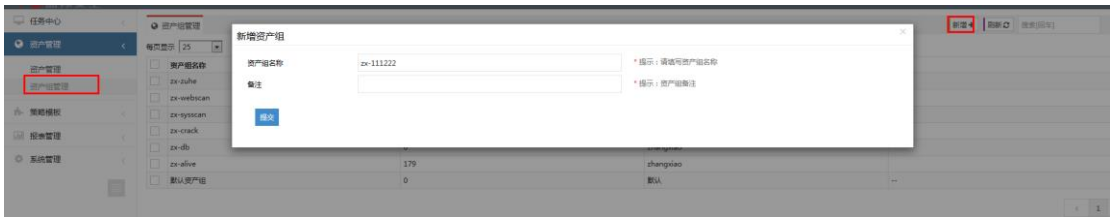


图 4.2.1-1 新增资产组

编辑资产组同理：选择已有的资产组->点击【编辑】->修改资产组名称后提交即可修改

4.2.2. 删除资产组

资产组删除包含了 2 种情况：资产组下无资产、资产组下有资产，当资产组下有资产时，删除资产组支持删除资产组及资产组下的资产或者仅删除资产组

- **仅删除资产组**

操作：在资产组管理页面->选择有资产的资产组，点击【删除】->选择仅删除资产组->提交，如下

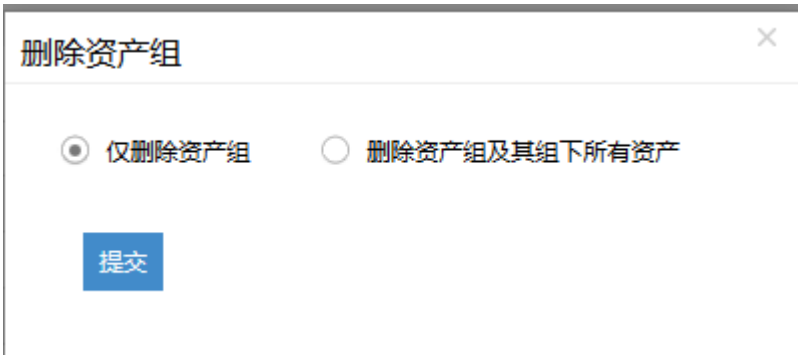


图 4.2.2-1 仅删除资产组

提交后，系统仅删除该资产组名称，资产组下的资产不会被删除，会同步到

默认资产组

- **删除资产组及其组下所有资产**

操作：在资产组管理页面->选择有资产的资产组，点击【删除】->选择删除资产组及其组下所有资产->提交，如下

图 4.2.2-2 删除资产组及组下所有资产

提交后，系统会将该资产组和资产组下的所有资产都删除

5. 策略模板

WEBUI：主界面 -> 策略模板

策略模块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 60000 多条，覆盖了 CVE、CNVD、CNNVD、CVEID、CNCVE、Bugtraq 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。

5.1.系统插件

WEBUI：主界面 -> 策略模板 -> 系统插件

系统插件包含了所有的漏洞插件，可以对插件策略模板、漏洞类别、漏洞进行相应的排序，查询。可通过搜索框搜索某一确定的漏洞名称、漏洞编号、CVE

号。如下图 6.1 所示：

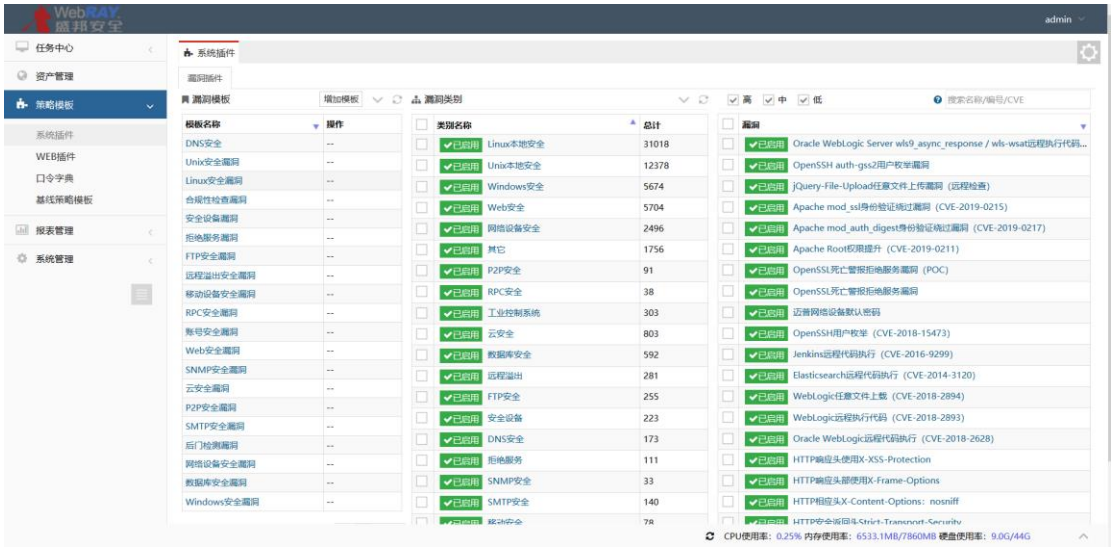


图 5.1 系统插件

5.1.1. 新增系统插件模板

用户除了可以使用系统默认提供的检测库模板外，也可以自定义规则库，我们提供了规则库模板的随意组合功能，可以有选择、有针对性的制定模板，确保检测的高效性。

点击【增加模板】，编写相应的系统插件模板名称即可新建成功。如图 5.1.1-1 所示：

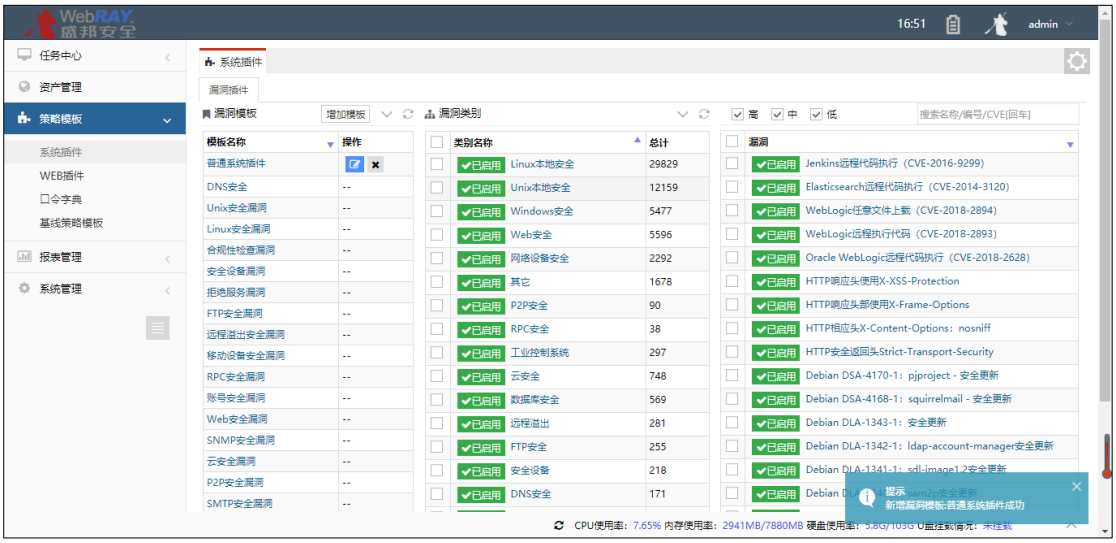


图 5.1.1-1 新增系统插件模板

新增插件模板成功后，默认包含所有的漏洞插件，选中该插件模板，可对某一漏洞类别插件或某一漏洞进行启用或者禁用设置，如图 5.1.1-2 所示：

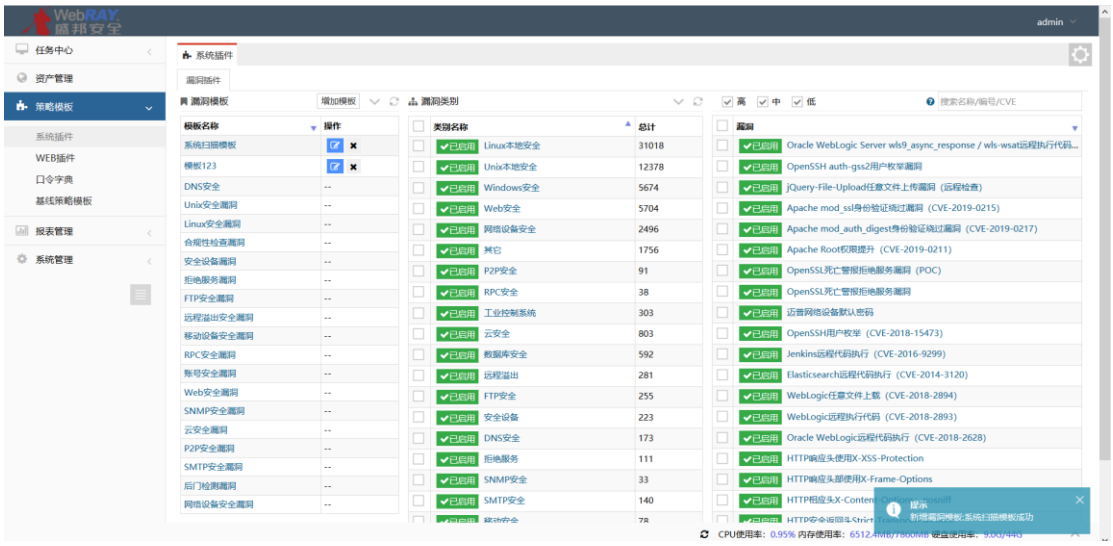


图 5.1.1-2 禁用插件

⚠：自定义插件模板可以进行相应的名称编辑、插件启用、禁用等，但系统默认的插件模板不能进行编辑、删除、以及启用或禁用某一插件。

5.2. Web 漏洞插件

WEBUI：主界面 -> 策略模板 -> 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。如图 5.2 所示：

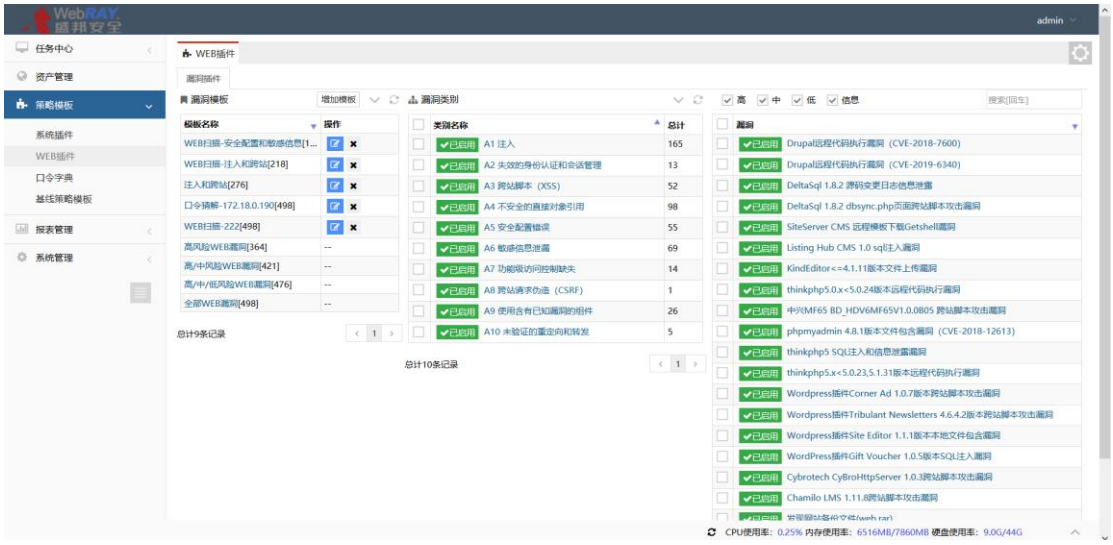


图 5.2 Web 插件

5.2.1. 新增 Web 插件模板

点击【增加模板】，填写相应的 Web 插件模板名称，点击【保存】按钮即可新建成功。如图 5.2.1-1 所示：

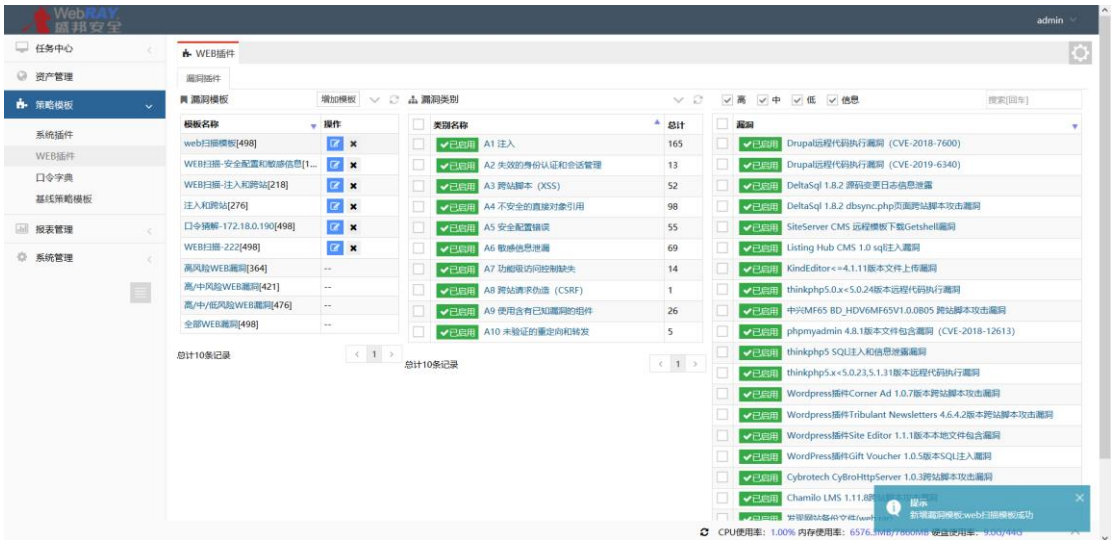


图 5.2.1-1 新增 Web 插件模板

新增插件模板成功后，默认包含所有的漏洞插件，选中该插件模板，可对某

一漏洞类别插件或某一漏洞进行启用或者禁用设置，如图 5.2.1-2 所示：

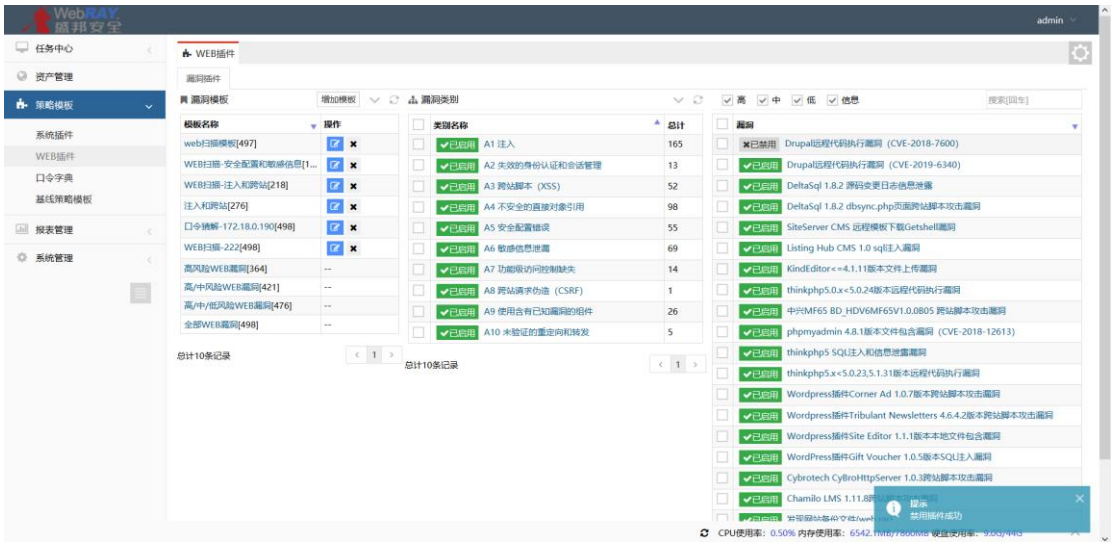


图 5.2.1-2 启用插件

5.3.口令字典

WEBUI：主界面 -> 策略模板 -> 口令字典

系统默认的有三种字典：组合字典，用户名字典，密码字典。组合字典中用户名和密码都有，主要是针对弱口令扫描时用户名和密码同时匹配才定义为弱口令。用户名字典和密码字典主要是弱口令扫描选择标准模式时对用户名和密码分开单独进行匹配。具体如图 5.3 所示：

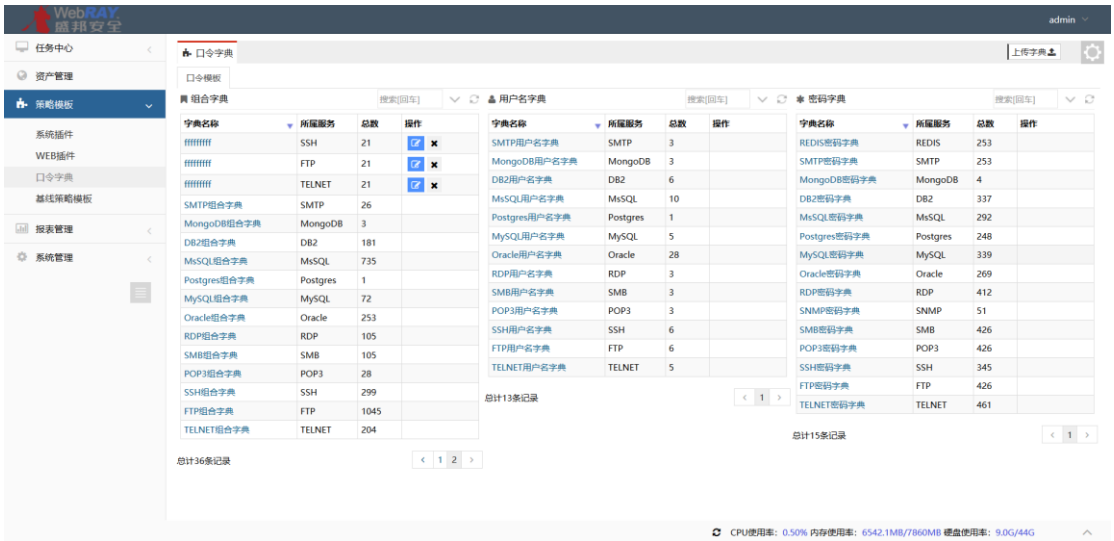


图 5.3 口令字典

5.3.1. 上传口令字典

用户可以自己上传弱口令字典，字典格式既可以为组合模式，也可以为标准模式，类型统一为 dic 格式，不支持其他类型的字典。具体如下图 5.3.1-1 所示：

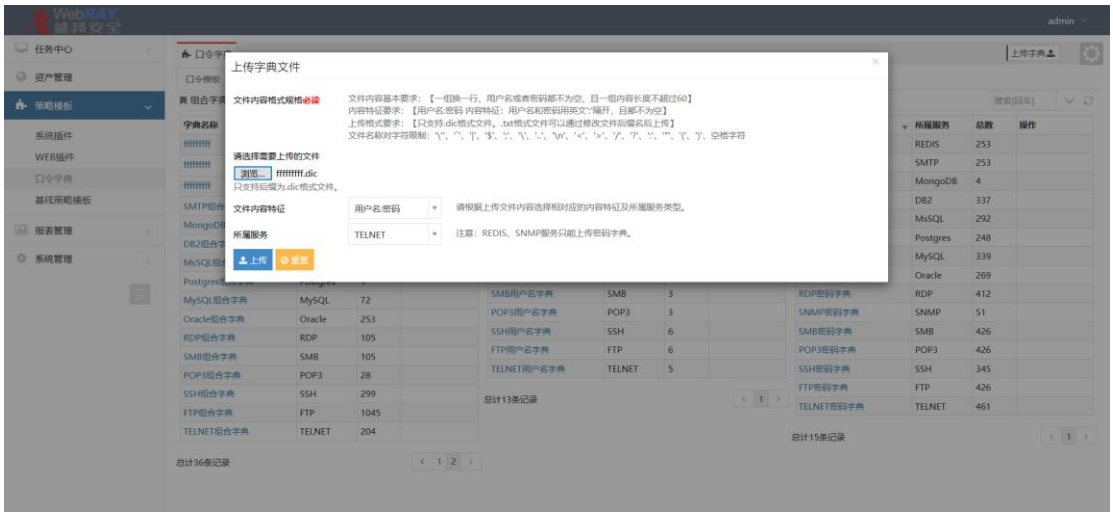


图 5.3.1-1 选择口令字典文件

选择要上传的弱口令字典文件，相应的文件内容特征，以及所属服务，点击【提交】即可上传成功。上传成功后界面如下图 5.3.1-2 所示：

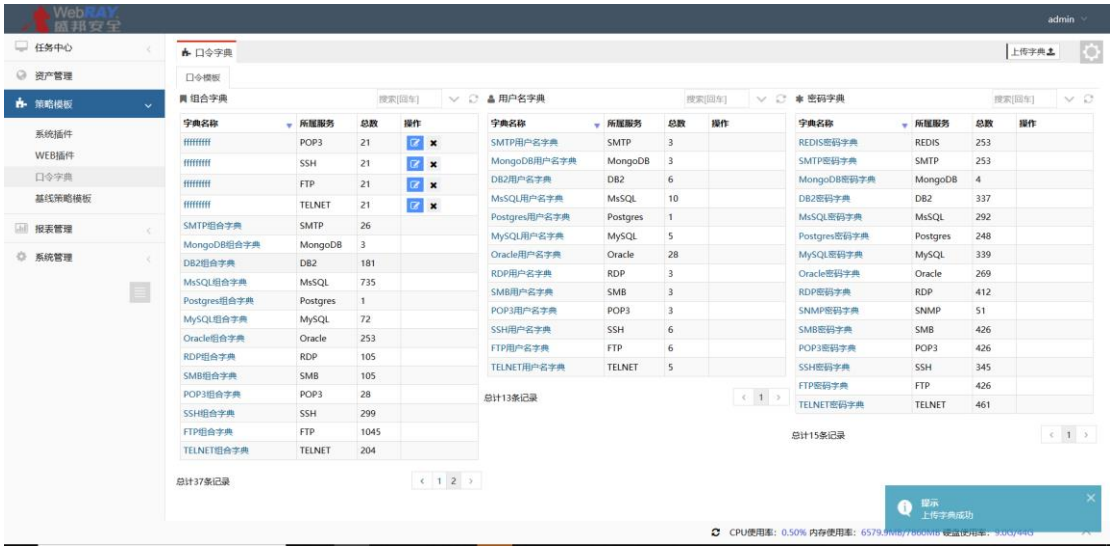


图 5.3.1-2 上传口令字典

5.4. 基线策略模板

WEBUI：主界面 -> 策略模板 -> 基线策略模板

安全基线核查功能主要是进行专业检查的，可以有效提高检查结果的准确性和合规性，用以在设备的上线安全检查、第三方入网安全检查、合规安全检查、日常安全检查和安全服务任务工作中。

预置的基线策略规则插件，可灵活自定义所需策略规则。具体的详情如下图 5.4 所示：

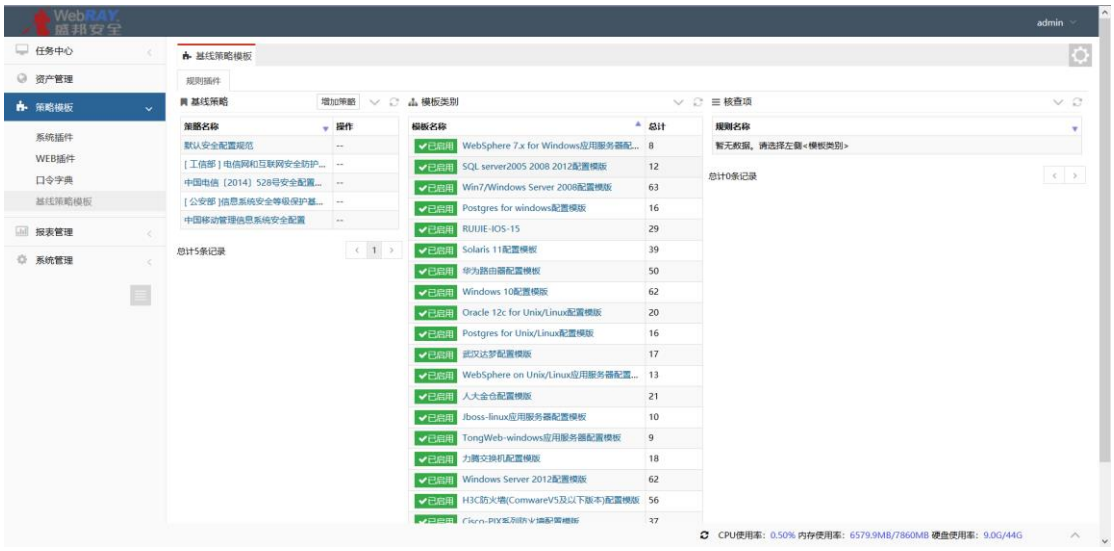


图 5.4 基线策略模板

5.4.1. 新建基线策略

点击【增加策略】，填写相应的基线策略名称，点击【保存】按钮即可新建成功。新增的基线策略默认包含所有插件，可通过“启用”“禁用”来进行插件的选择。如图 5.4.1 所示

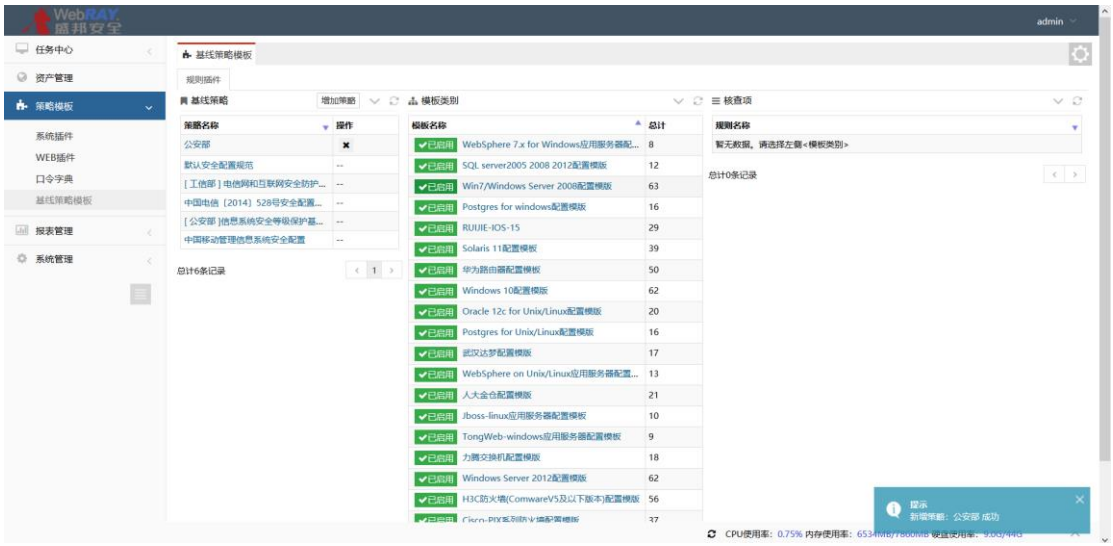


图 5.4.1 新建基线策略

6. 报表管理

6.1.数据查询

WEBUI：主界面 -> 报表管理 ->数据查询

数据查询模块可以查看主机 IP 和 web 资产漏洞情况，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，当任务以及漏洞数目较多且查找不方便时，支持根据任务名称或漏洞名称进行搜索和排序。

6.1.1. 资产漏洞查询

资产漏洞支持多个维度的查询及组合查询，从查询出的漏洞列表中可查看漏洞对应的资产、漏洞分类、漏洞等级、梳理、端口/服务和漏洞评分信息，且查询出的漏洞列表支持导出

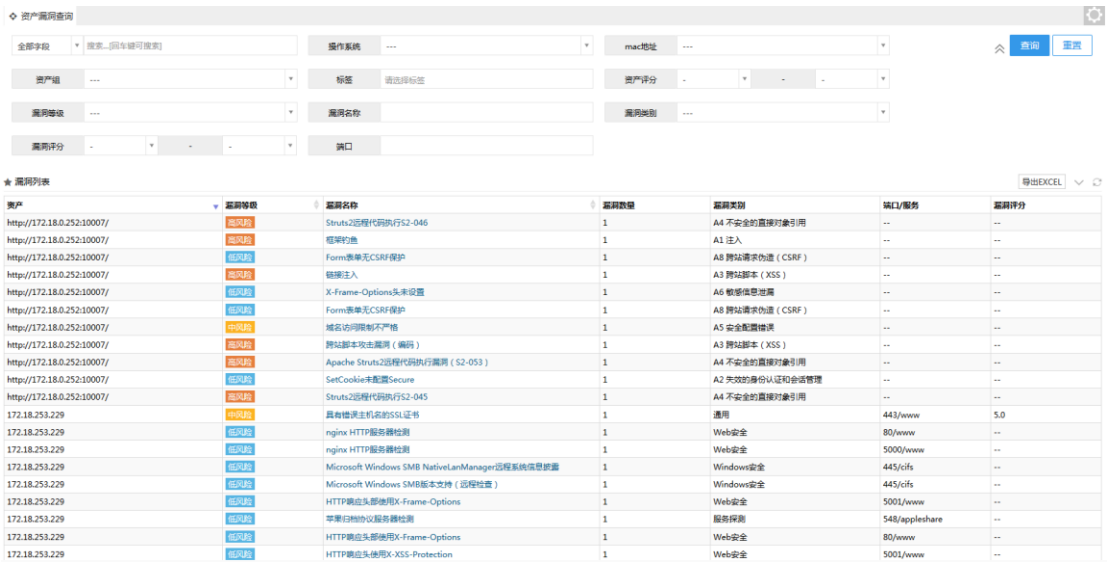


图 6.1.1-1 数据查询

支持的查询参数如下：

表 6.1.1-1 数据查询条件参数说明

参数	描述
资产名称	主机资产或者web资产名称
资产 ip	主机资产的ip
资产 url	Web资产的url
服务器信息	Web资产使用的服务器信息
网页编码	Web资产使用的网页编码技术
服务器语言	Web资产使用的服务器语音
物理地址	资产设备所在的物理地址
操作系统	主机设备的操作系统类型
Mac 地址	主机设备的mac地址
资产组	资产所属的资产组，下发任务时指定或者新增资产时指定
标签	资产标签，由用户定义

资产评分	资产经过扫描后的系统给出的风险值，风险值越高说明资产越不安全
漏洞名称	主机或web网站检测出的漏洞名称
漏洞等级	检测出的漏洞对应的危险等级，分为“高、中、低、信息”
端口	主机设备检测出的漏洞对应的端口
漏洞类别	检测出的漏洞对应的漏洞类别

具体查询操作如下：

1) 进入资产管理界面->点击，展开所有搜索条件

2) 配置不同查询参数->点击查询，查看符合条件的漏洞信息

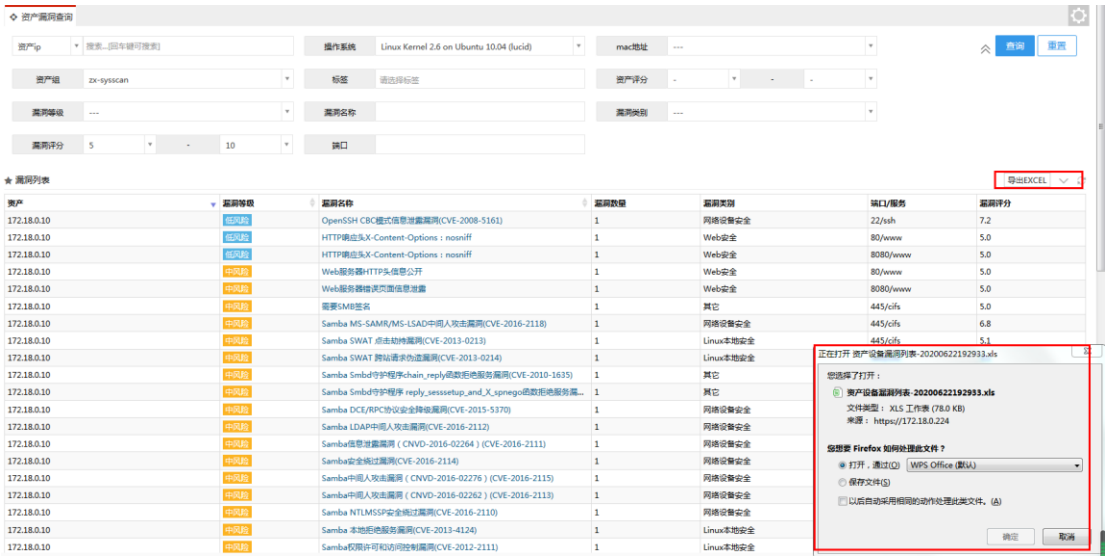
3) 单击【重置】按钮，可以清空查询条件，重新查询漏洞信息。

图 6.1.1-12 数据查询

6.1.2. 资产漏洞导出

对于搜索出符合条件的漏洞信息，可进行导出，操作如下：

在资产漏洞查询页面->按条件搜索漏洞->点击导出，即可将符合条件的漏洞信息以 excel 格式导出



资产	漏洞等级	漏洞名称	漏洞数量	漏洞类别	端口/服务	漏洞评分
172.18.0.9	低风险	OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161)	1	网络设备安全	22/ssh	7.2
172.18.0.9	低风险	HTTP响应头X-Content-Options：nosniff	1	Web安全	80/www	5.0
172.18.0.9	低风险	HTTP响应头X-Content-Options：nosniff	1	Web安全	8080/www	5.0
172.18.0.9	中风险	Web服务器HTTP头信息公开	1	Web安全	80/www	5.0
172.18.0.9	中风险	Web服务器错误页面信息泄露	1	Web安全	8080/www	5.0
172.18.0.9	中风险	需要SMB签名	1	其它	445/cifs	5.0
172.18.0.9	中风险	Samba MS-SAMR/MS-LSAD中间人攻击漏洞(CVE-2016-2118)	1	网络设备安全	445/cifs	6.8
172.18.0.9	中风险	Samba SWAT 点击劫持漏洞(CVE-2013-0213)	1	Linux本地安全	445/cifs	5.1
172.18.0.9	中风险	Samba SWAT 跨站请求伪造漏洞(CVE-2013-0214)	1	Linux本地安全	445/cifs	5.1
172.18.0.9	中风险	Samba Smbd守护程序chain_reply函数拒绝服务漏洞(CVE-2010-1635)	1	其它	445/cifs	5.0
172.18.0.9	中风险	Samba Smbd守护程序reply_sesssetup_and_X_spnego函数拒绝服务漏洞(CVE-2010-1642)	1	其它	445/cifs	5.0

图 6.1.2-1 资产漏洞导出

6.2.对比分析

WEBUI：主界面 -> 报表管理 ->对比分析

6.2.1. 资产对比分析

漏洞变化对比分析：用户可以针对同一资产不同检测时间段的扫描结果进行对比分析，可以查看漏洞趋势变化图以及统计出新增和减少的漏洞。如图 6.2.1-1 所示：

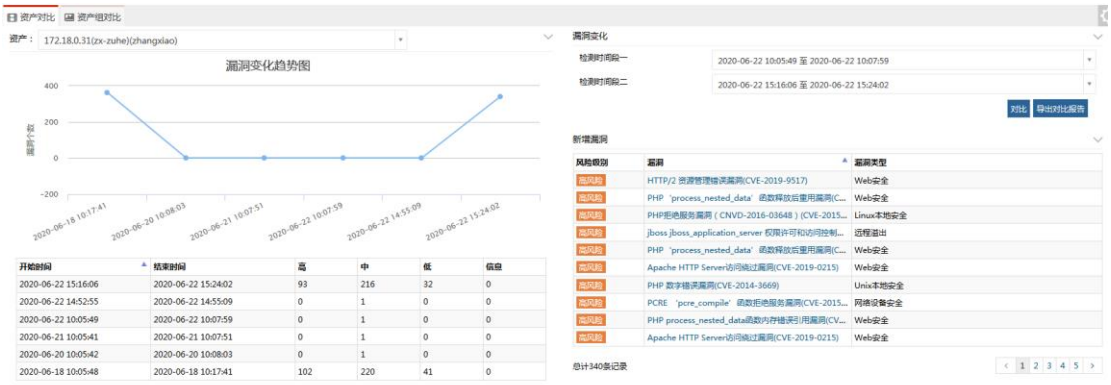


图 6.2.1-1 资产漏洞对比分析

资产组对比分析：用户可对多个资产组进行漏洞统计对比分析，查看资产组间漏洞情况。具体情况如下图所示：

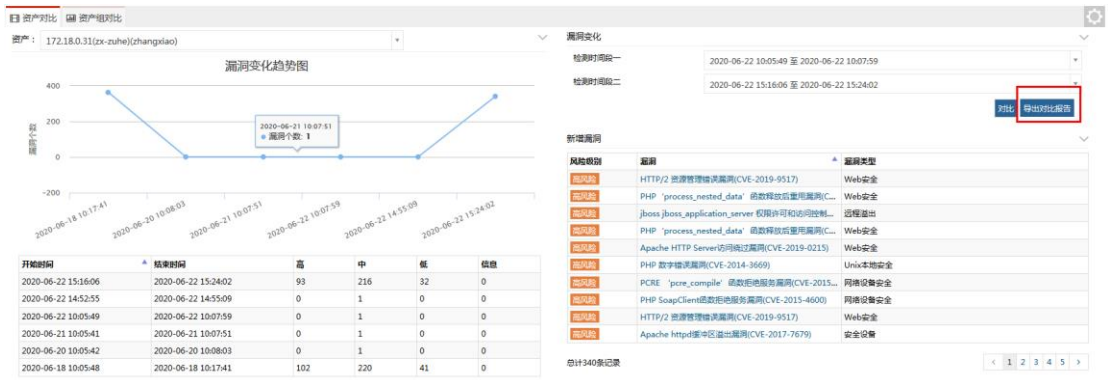
图 6.2.1-2 资产组对比分析

6.2.2. 导出对比报告

资产漏洞对比和资产组对比数据支持导出到 excel 进行查看

- **导出资产对比报告**

操作：点击对比分析->资产对比->进入资产对比页面->选择资产->点击对比->点击导出对比报告，如下



资产：	172.18.0.31	
检测时间段一	2020-06-22 10:05:49至2020-06-22 10:07:59	
检测时间段二	2020-06-22 15:16:06至2020-06-22 15:24:02	
新增漏洞		
风险级别	漏洞	漏洞类型
高风险	HTTP/2 资源管理错误漏洞(CVE-2019-9517)	Web安全
高风险	PHP ‘process_nested_data’ 函数释放后重用漏洞	Web安全
高风险	jboss jboss_application_server 权限许可和访问控	远程溢出
高风险	PHP ‘process_nested_data’ 函数释放后重用漏洞	Web安全
高风险	Apache HTTP Server访问绕过漏洞(CVE-2019-	Web安全
高风险	PHP 数字错误漏洞(CVE-2014-3669)	Unix本地安全
高风险	PCRE ‘pcre_compile’ 函数拒绝服务漏洞(CVE-	网络设备安全
高风险	PHP SoapClient函数拒绝服务漏洞(CVE-2015-	网络设备安全
高风险	HTTP/2 资源管理错误漏洞(CVE-2019-9517)	Web安全
高风险	Apache httpd缓冲区溢出漏洞(CVE-2017-7679)	安全设备
高风险	SQLite拒绝服务漏洞（CNVD-2015-02750）(CVE-	Unix本地安全
高风险	PHP远程代码执行漏洞（CNVD-2015-06226）	Linux本地安全
高风险	PHP存在多个远程代码执行漏洞(CVE-2015-6834)	网络设备安全
高风险	Apache HTTP Server访问绕过漏洞(CVE-2019-	Web安全
高风险	SQLite拒绝服务漏洞（CNVD-2015-02748）(CVE-	云安全
高风险	PCRE拒绝服务漏洞（CNVD-2015-07884）(CVE-	网络设备安全
高风险	PHP SOAP访问远程内存破坏漏洞(CVE-2015-	网络设备安全

图 6.2.2-1 资产对比报告导出

- **导出资产组对比报告**

操作：点击对比分析->资产组对比->进入资产组对比页面->选择不同的资产组->点击对比->点击导出对比报告，如下

资产组一	zx-zuhe					
资产组二	zx-sysscan					
对比统计						
资产组名称	资产总数	漏洞总数	高危漏洞	中危漏洞	低危漏洞	信息
zx-zuhe	1	341	93	216	32	0
zx-sysscan	75	2360	433	1490	434	3

图 6.2.2-2 资产组对比报告导出

6.3.导出报表

WEBUI：主界面 -> 报表管理 ->导出报表

报表导出主要是针对多个用户角色生成多种类型的报表，以图、表、文字描述相结合的方式展示给用户。

6.3.1. 输出报表

用户可将漏洞扫描结果以报表的形式进行输出。可选择导出对象、资产组以及检测任务时间段。导出格式提供了 HTML，WORD，PDF ,EXCEL，XML 五种格式，导出方式分为详细报告和统计报表，报表标题可自定义，导出文件名默认同步资产名称，也可对其进行自定义，报表内容支持使用报表模板进行自定义，也支持压缩包加密功能。

导出报表操作如下：

1） 选择菜单导出报表->导出报表，进入报表导出页面，如下

图 6.3.1-1 导出报表

2) 选择配置导出的报表参数，如下

表 6.3.1-1 导出报表参数说明

参数	说明
选择导出对象	可选择按照任务或者按照资产导出报表
指定任务列表/资产	可选择任务和已生成的资产
导出格式	支持 HTML、WORD、EXCEL、PDF、XML 五种报表格式
导出方式	分为详细报表和统计报表两种
报表标题	可自定义报表标题，也可使用默认标题
导出文件名	可自定义导出文件名，也可使用默认名称
设置压缩报密码	导出报表压缩包支持设置压缩密码，通常在涉密机构使用

3) 点击导出，界面上方显示导出进度条，在报表导出过程中，若要停止导出，点击进度条上的 x 即可

图 6.3.1-2 导出报表进度条

4） 报表导出成功后可直接选择保存到本地或者直接打开，如下

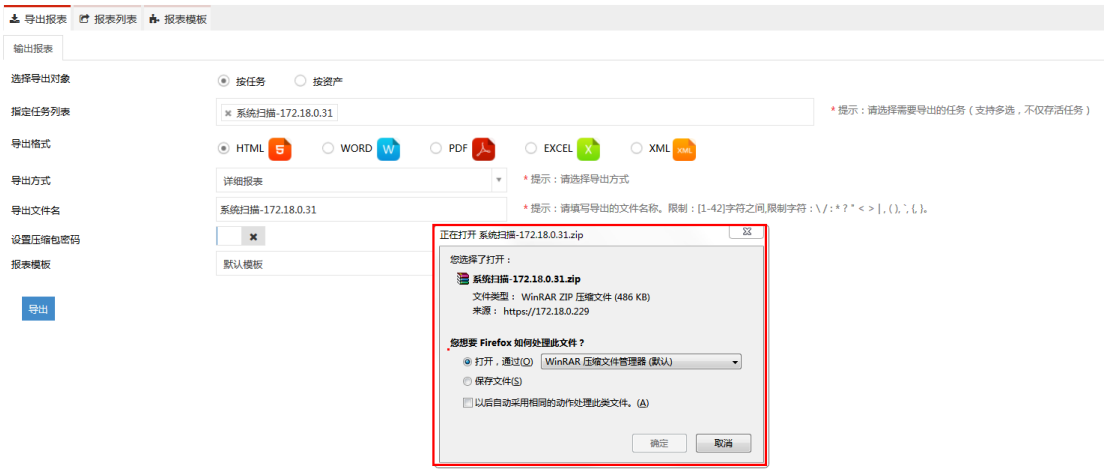


图 6.3.1-3 导出报表完成

6.3.2. 报表列表

报表列表是将导出的报表直接同步到报表列表里，报表列表可以展示导出的报表名称以及生成日期，报表名称默认包含扫描类型、资产以及报表格式。报表格式可以存储多个报表文件，若报表列表里面报表较多，查找不方便，可通过搜索名称来进行搜索。对于报表文件支持批量删除，以及单报表删除。具体详情如下图 6.3.2 所示

图 6.3.2-1 报表列表

- **历史报表下载**

操作：在报表列表页面->选择历史报表->点击下载->即可将历史报表重新下载到本地，如下图：

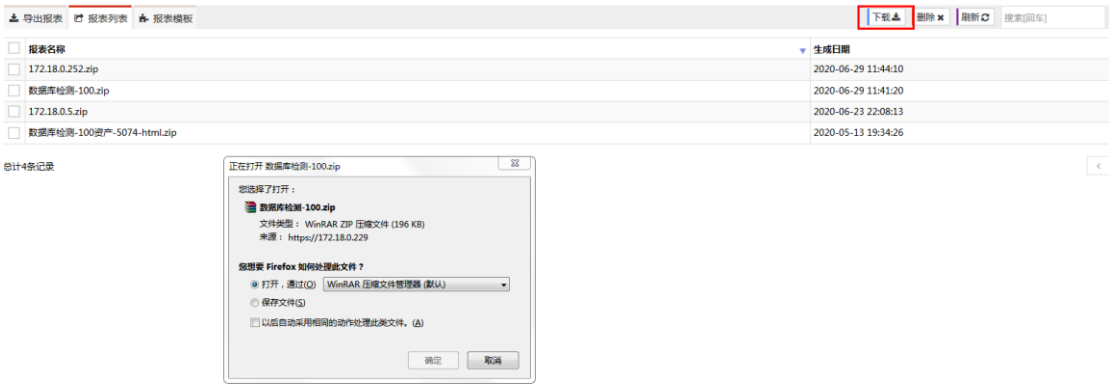


图 6.3.2-2 历史报表下载

- **历史报表删除**

操作：在报表列表页面->选择历史报表->点击删除->即可将历史报表删除，如下图：

图 6.3.2-3 历史报表删除

- **历史报表搜索**

操作：在报表列表页面->在搜索框中按照报表名称搜索，支持模糊搜索

6.3.3. 报表详情

资产报表内容由主机资产和主机上的 web 资产信息组成，报表数据来自系统扫描、web 扫描、口令猜解、存活探测扫描任务的扫描结果；报表按内容分为统计报表和详细报表

6.3.3.1. 统计报表

统计报表：内容包括按任务或者按资产导出的经扫描后的数据统计信息，如检测结果综述、任务概览、漏洞统计、敏感端口/服务/中间件、漏洞分布、类别统计等。具体详情如下图所示：

漏洞扫描安全评估报告

1 检测结果综述

本次检测中，扫描了1个主机，2个站点。
检测到漏洞共148个，系统漏洞133个，Web漏洞15个。高危漏洞共13个，中危漏洞共103个，低危漏洞共26个，信息级漏洞共6个。
检测到弱口令共1个。
整体风险等级为比较危险，非常危险的资产共1个，需重点关注。

2 任务总体概览

2.1 任务基本信息

任务名称	172.18.0.31
扫描目标	172.18.0.31
报表模板	默认模板
任务所在账号	
扫描时间	开始时间：【2020-06-23 19:53:53】结束时间：【2020-06-23 20:45:32】(耗时：51分39秒)
系统版本	V3.0(4.0.1-R1-v62970-20200623)
规则库版本	20200628094338

2.2 整体漏洞统计

以IP为维度，覆盖主机IP以及该IP上存在的Web站点，整体进行漏洞统计，统计结果如下表所示：

序号	IP（域名）	高	中	低	信息	总计（次）
1	172.18.0.31	13	103	26	6	148

2.3 敏感端口/服务

本次任务检测到开放了以下【1】种敏感端口或服务，开放最多的端口为【22】端口，对应【1】个资产，具体情况如下表所示。

序号	端口	服务	协议	主机
1	22	ssh	TCP	172.18.0.31

说明：敏感端口/服务指根据安全研究表明，容易被黑客利用漏洞发起攻击的端口/服务。

2.4 敏感中间件

本次任务检测到以下1种敏感中间件，其中使用最多的中间件是【Apache/2.4.7 (Ubuntu)】，具体情况如下表所示：

序号	中间件	网站
1	Apache/2.4.7 (Ubuntu)	http://172.18.0.31:10004/ http://172.18.0.31:10005/

目录

4.1.2 WEB漏洞影响资产分布

影响Web资产最多的漏洞是【域名访问限制不严格】，共有【2】个Web站点中存在该漏洞，漏洞等级为【中风险】。漏洞影响资产数量TOP10分布如下图所示：

Web漏洞影响Web资产情况如下表所示：

序号	漏洞名称	漏洞分组	受影响资产
1	域名访问限制不严格	A5 安全配置错误	http://172.18.0.31:10005/ http://172.18.0.31:10004/
2	发现内网IP地址	A6 敏感信息泄漏	http://172.18.0.31:10005/ http://172.18.0.31:10004/
3	X-Frame-Options头未设置	A6 敏感信息泄漏	http://172.18.0.31:10005/ http://172.18.0.31:10004/
4	Apache服务存在多个安全漏洞	A6 敏感信息泄漏	http://172.18.0.31:10005/ http://172.18.0.31:10004/
5	服务器版本信息泄漏	A6 敏感信息泄漏	http://172.18.0.31:10005/ http://172.18.0.31:10004/
6	启用了危险的Method	A5 安全配置错误	http://172.18.0.31:10005/
7	Form表单无CSRF保护	A8 跨站请求伪造（CSRF）	http://172.18.0.31:10005/
8	敏感文件或备份	A5 安全配置错误	http://172.18.0.31:10005/

目录

图 6.3.3.1-1 统计报表内容

：html、word、pdf 格式报表内容相同，只是以不同形式展示出来，建议用户导出报表为 html，排版更加直观美观。

6.3.3.2. 详细报表

详细报表：导出的详细报表压缩包中包含所选任务或者所选资产的统计报表和每个资产的详细报表，详细报表中展示了资产和任务的详细信息，如资产检测时间、检测结果详情、资产属性信息、详细的漏洞描述信息等，如下图所示：

WebRAY 盛邦安全

漏洞扫描安全评估报告

1 检测结果综述

本次报告中，目标【172.18.0.31】共检测出风险148个，其中系统漏洞133个，Web漏洞15个，弱口令1个。

整体风险值为7.2，安全等级为比较危险。所有漏洞中，高危漏洞13个，中危漏洞103个，低危漏洞26个，信息级漏洞6个。（漏洞风险等级的分类规则及资产风险等级分类规则，请参见章节《资产风险等级评定标准》）。

2 资产总体概览

2.1 资产基本信息

系统资产列表：

主机名称	172.18.0.31
主机资产	172.18.0.31
操作系统	Linux Kernel 4.15 on Ubuntu 18.04 (bionic)
MAC地址	
扫描时间	开始时间：【2020-06-23 20:27:23】结束时间：【2020-06-23 20:45:32】(耗时：18分9秒)
资产风险值	9.6
漏洞分布	漏洞总计：133 高风险：13 中风险：101 低风险：19
漏洞状态标识	新增：133 误报：0 已修复：0
资产组	zx-zuhe
标签	
系统版本	V3.0(4.0.1-R1-v62970-20200623)
规则库版本	20200628094338

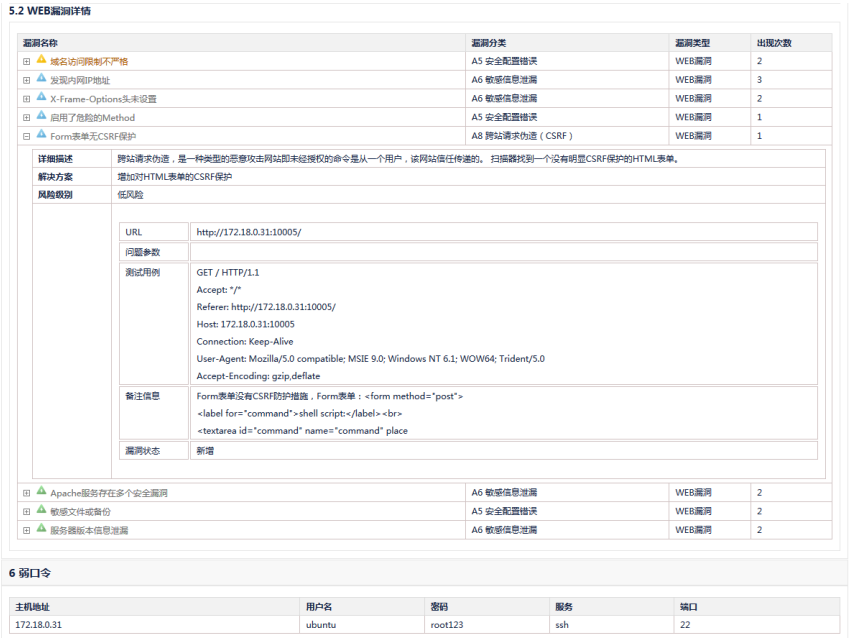
WEB资产列表：

Web资产	http://172.18.0.31:10004/
网站域名	172.18.0.31
IP地址	172.18.0.31
服务器信息	Apache/2.4.7 (Ubuntu)
网站标题	403Forbidden

目录

4.2 主机漏洞详情

漏洞名称	漏洞分类	漏洞类型	出现次数
Apache httpd缓冲区溢出漏洞(CVE-2017-7679)	安全设备	高风险	2
漏洞编号	107499		
风险级别	高风险		
概要			
描述	Apache httpd是美国阿帕奇（Apache）软件基金会的一款专为现代操作系统开发和维护的开源HTTP服务器。 Apache httpd 2.2.33之前的2.2.x版本和2.4.26之前的2.4.x版本存在安全漏洞。攻击者可利用该漏洞造成缓冲区越边界读取。		
解决办法	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://lists.apache.org/thread.html/f4515e580dfb6eeca589a5cdebd4c4c709ce632b12924f343c3b7751		
详情请参阅	http://www.securityfocus.com/bid/99170		
CVE	CVE-2017-7679		
Bugtraq ID	99170		
CVSS	CVSS2: 7.5(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P);		
CNVD	CNVD-2017-7679		
CNCVE	CNCVE-2017-7679		
检测详情	主机：172.18.0.31 | 端口：10005 | 服务：www | 协议：tcp 漏洞状态：新增 主机：172.18.0.31 | 端口：10004 | 服务：www | 协议：tcp 漏洞状态：新增		
HTTP/2 资源管理错误漏洞(CVE-2019-9517)	Web安全	高风险	2
Apache httpd拒绝服务漏洞（CNVD-2017-11803）(CVE-2017-7668)	安全设备	高风险	2
Apache HTTP Server本地权限提升漏洞(CVE-2019-0211)	Web安全	高风险	2
Apache HTTP Server拒绝服务漏洞（CNVD-2017-11802）(CVE-2017-3169)	安全设备	高风险	2
Apache httpd身份验证绕过漏洞(CVE-2017-3167)	安全设备	高风险	2
OpenSSH用户枚举（CVE-2018-15473）【POC】	其它	高风险	1
Apache HTTP Server 授权问题漏洞(CVE-2018-17199)	Linux本地安全2	中风险	2
Web服务器HTTP头信息公开	Web安全	中风险	2



5.2 WEB漏洞详情

漏洞名称	漏洞分类	漏洞类型	出现次数
域名访问限制不严格	A5 安全配置错误	WEB漏洞	2
发现内网IP地址	A6 敏感信息泄漏	WEB漏洞	3
X-Frame-Options头未设置	A6 敏感信息泄漏	WEB漏洞	2
启用了危险的Method	A5 安全配置错误	WEB漏洞	1
Form表单无CSRF保护	A8 跨站请求伪造（CSRF）	WEB漏洞	1
详细描述	跨站请求伪造，是一种类型的恶意攻击网站即未经授权的命令是从一个用户，该网站信任传递的。 扫描器找到一个没有明显CSRF保护的HTML表单。		
解决方案	增加对HTML表单的CSRF保护		
风险级别	低风险		
URL	http://172.18.0.31:10005/		
问题参数			
测试用例	GET / HTTP/1.1 Accept: */* Referer: http://172.18.0.31:10005/ Host: 172.18.0.31:10005 Connection: Keep-Alive User-Agent: Mozilla/5.0 compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0 Accept-Encoding: gzip,deflate		
备注信息	Form表单没有CSRF防护措施，Form表单：<form method="post"> <label for="command">shell script:</label> <textarea id="command" name="command" place		
漏洞状态	新增		
Apache服务存在多个安全漏洞	A6 敏感信息泄漏	WEB漏洞	2
敏感文件或备份	A5 安全配置错误	WEB漏洞	2
服务器版本信息泄漏	A6 敏感信息泄漏	WEB漏洞	2

6 弱口令

主机地址	用户名	密码	服务	端口
172.18.0.31	ubuntu	root123	ssh	22

7 参考标准

7.1 单一漏洞风险等级评定标准

危险程度	危险值区域	危险程度说明
高	7 <= 漏洞风险值 <= 10	攻击者可以远程执行任意命令或者代码，或对系统进行远程拒绝服务攻击。
中	4 <= 漏洞风险值 < 7	攻击者可以远程创建、修改、删除文件或数据，或对普通服务进行拒绝服务攻击。
低	0 <= 漏洞风险值 < 4	攻击者可以获取某些系统、服务的信息，或读取系统文件和数据。

1. 可远程获取漏洞组件的版本信息。
2. 目标系统服务器开放了不必要的服务。
3. 可远程访问到某些不在目录树中的文件或读取服务器动态脚本的源码。
4. 可远程因为会话管理的问题导致身份冒用。
5. 可远程利用受影响的系统服务器攻击其他浏览网站的用户。
6. 可远程读取系统文件或后台数据库。
7. 可远程读写系统文件、操作后台数据库。
8. 可远程以普通用户身份执行命令或进行拒绝服务攻击。
9. 可远程以管理用户身份执行命令（受限、不太容易利用）。
10. 可远程以管理用户身份执行命令（不受限、容易利用）。

7.2 资产风险等级评定标准

资产风险等级	资产风险值区域
非常危险	8 <= 资产风险值 <= 10
比较危险	5 <= 资产风险值 < 8
比较安全	2 <= 资产风险值 < 5
非常安全	0 <= 资产风险值 < 2

1. 将资产的漏洞按照分数的高低排序，依据漏洞的分数将漏洞威胁划分为高、中、低三个类别。
2. 单个资产的风险值按照风险评估模型计算来得到；网络的风险值是由最危险资产决定，即最大的资产风险值。
3. 高、中、低漏洞威胁的定义参见《单一漏洞风险等级评定标准》。
4. 资产的风险等级定位为四级：非常危险、比较危险、比较安全和非常安全。具体的评判标准请参考《资产风险等级评定标准》。

8 安全建议

随着越来越多的网络访问通过系统漏洞进行操作，系统漏洞已成为互联网安全的一个热点，基于系统漏洞的攻击广为流行，CGI攻击检测、网络设备和防火墙、本地安全检查等问题严重威胁着系统管理者和系统用户的安全，我们有必要采取措施消除这些风险。

建议对存在漏洞的资产参考附件中提出的解决方案进行漏洞修补、安全增强。

请专业的安全研究人员或安全公司对系统架构做全面的安全审计，修补所有发现的安全漏洞；这种白盒安全测试比较深入全面。

对系统的开发人员进行安全编码方面的培训，在开发过程避免漏洞的引入能起到事半功倍的效果。

采用专业的系统安全产品，可以在不修改系统本身的情况下对大多数的基于漏洞攻击起到有效的阻断作用。

建议网络管理员、系统管理员、安全管理员关注安全信息、安全动态及最新的高危漏洞，特别是影响到漏洞站点所使用的系统和软件的漏洞，应该在事前设计好应对规划，一旦发现系统受漏洞影响及时采取措施。

目录

图 6.3.3.2-1 详细报表内容

6.3.4. 报表模板

通过新增报表模板用户可以自定义生成的报表中显示的内容。系统自带了默认模板，默认模板中所有章节内容都开放，不可编辑和删除。

6.3.4.1. 新建报表模板

- **自定义漏洞等级、漏洞状态、公司信息、报表标题**

操作：（1）点击报表管理->导出报表->报表模板，进入报表模板页面->点击新增，配置模板名字、需要导出的漏洞等级、漏洞状态、公司信息、报表标题，提交，如下：

图 6.3.4.1-1 自定义报表模板

操作：（2）在导出报表页面->选择任务或资产->下拉选择自定义的报表模板->导出，导出的报表内容即和选择的模板一致。如下

图 6.3.4.1-2 选择自定义报表模板导出报表

- **自定义报表章节**

操作：（1）点击报表管理->导出报表->报表模板，进入报表模板页面->点击新增，配置模板名字、开启自定义报表章节->选择报表中要展示的章节，提交，如下：

图 6.3.4.1-3 自定义报表章节

操作：（2）在导出报表页面->选择任务或资产->下拉选择自定义的报表模板->导出，导出的报表内容即和选择的模板一致。如下

图 6.3.4.1-3 选择自定义报表章节导出

6.3.4.2. 报表模板操作

- **编辑**

操作：选择模板->点击编辑按钮，编辑模板内容后->点击提交，完成模板编辑

➢ **删除**

操作：选择模板->点击删除按钮->点击确认，即可删除自定义的模板

7. 系统管理

7.1.账号管理

7.1.1. 修改密码

：所有用户均有修改密码的权限。

选择“系统管理->账户管理”，默认进入修改密码页面。修改密码必须输入正确的旧密码，如果旧密码输入错误，则不允许修改密码。修改密码成功后，将在下次登陆时要求输入新的密码。

具体详情如下图 7.1.1 所示

图 7.1.1 修改密码

修改密码配置参数说明如表 7.1.1 所示

表 7.1.1 配置参数说明

参数	说明
旧密码	管理用户需要修改的原始密码
新密码	管理用户设置的新密码
确认新密码	重新输入新密码，确认一致性

⚠注意：请牢记修改后的密码，如果忘记系统密码，将不能登录系统。

7.2.诊断工具

WEBUI：主界面 -> 系统管理 ->诊断工具

7.2.1. 网络诊断

7.2.1.1. PING 命令

PING 命令用于检测主机存活或网络通断情况，在输入框中输入 IP 地址或者域名会列出执行结果。PING 命令支持 ipv4 和 ipv6 的诊断，如图 7.2.1.1-1 所示：

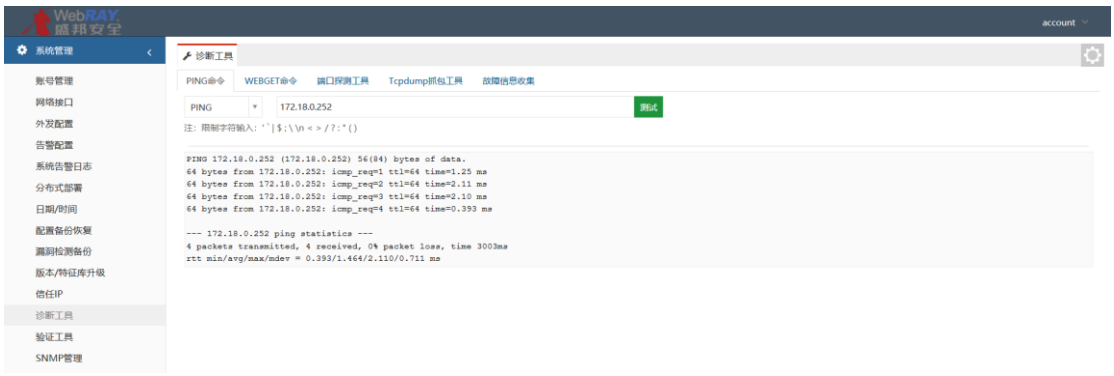


图 7.2.1.1-1 诊断工具-PING 命令

7.2.1.2. WGET 命令

用 WGET 命令测试扫描器和网站首页的连通性，如图 7.2.1.2-1 所示：

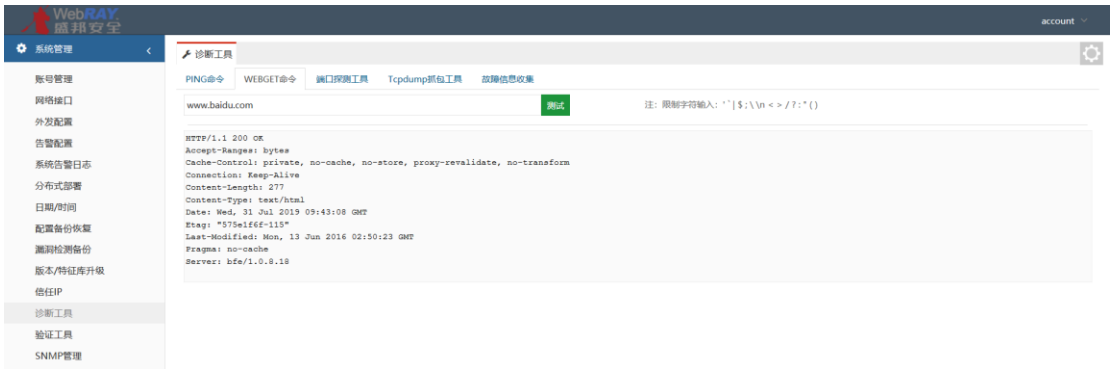


图 7.2.1.2-1 诊断工具-WGET 命令

7.3.验证工具

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，可以直接利用验证工具手动添加 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，通用验证如图 7.3-1 所示，SQL 注入验证如图 7.3-2 所示。

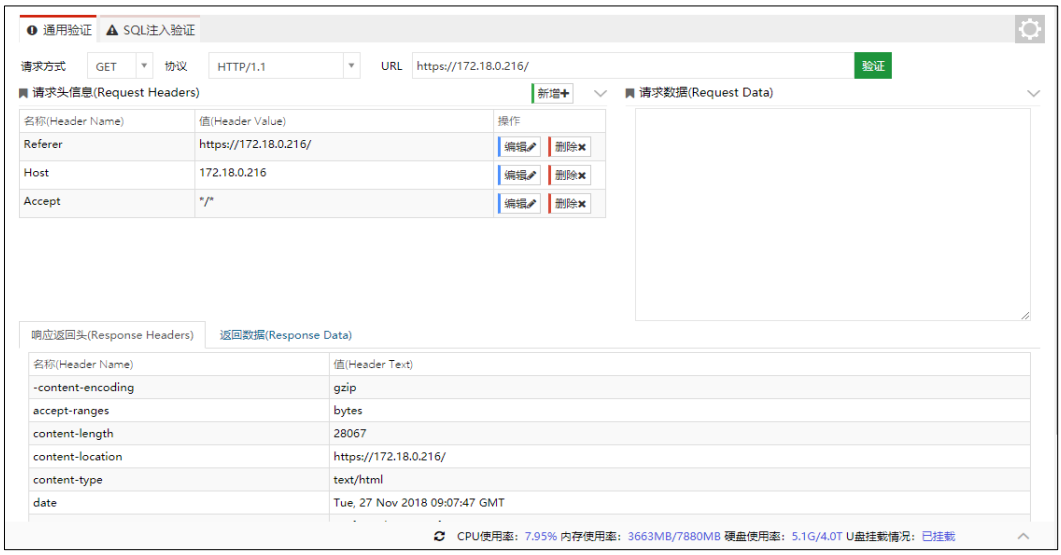


图 7.3-1 通用验证

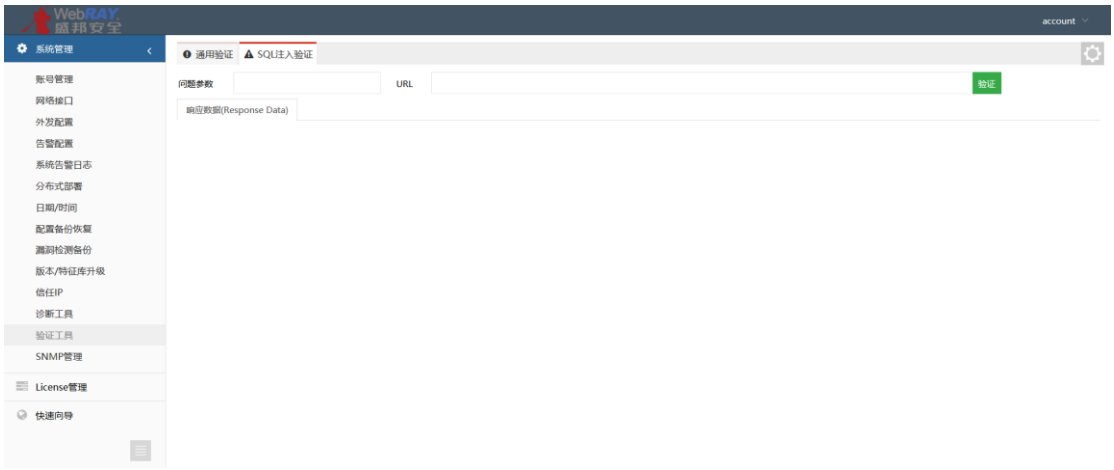


图 7.3-2 SQL 注入验证

远江盛邦（北京）网络安全科技股份有限公司

地址：北京市海淀区农大南路硅谷亮城 2 号楼 A 座 6 层

电话：010-82730576

传真：010-82730577

服务：4006-911-199

网址：http://www.webray.com.cn