

羚见数据安全检查工具箱 SEC6000-RAS-DCBox

用户手册



版本: V6.0.3.1 (20240703)

密级: 受限公开

■ 版权声明

本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容,除另有特别注明,版权均属 杭州领信数科信息技术有限公司(简称领信数科)所有,受到有关产权及版权法保护。任何个人、机构 未经领信数科的书面授权许可,不得以任何方式复制或引用本文的任何片断。

■ 内容声明

您购买的产品、服务或特性等受合同和条款的约束,本文档中描述的部分功能可能不在您的购买或使用范围之内。

本文档仅作为使用指导,实际产品可能会由于版本升级或其他原因,与文档描述有略微差异。

■ 免责声明

在使用产品之前,请详细阅读免责声明,一旦开始使用,即认可和接受本声明的全部内容。在使用过程 中,领信数科不对以下情况承担任何责任:

•因系统运维或管理人员未及时处理影响系统稳定性和可用性的告警,而造成的数据损失、系统可用性降低等情况。

•因业务量超过所规划硬件能力而造成的数据损失、系统可用性降低等情况。

•因自然灾害(包含但不限于水灾、火灾、地震等)或外部原因(包含但不限于断网、断电等)而造成的 数据损失、系统可用性降低或不可用等情况。

■ 格式约定

•粗体字:菜单、命令和关键字

•斜体字: 文档名、变量

•说明:对描述内容的补充和引用信息





•警告:有可能造成人身伤害的警告信息



目 录

前	音	6
	内容简介	6
	获得帮助	6
─.	产品概述	7
	1.1 背景	7
	1.2 体系结构	7
	1.3 部署方式	8
	1.4 产品定位	9
	1.4.1 资产管理	9
	1.4.2 脆弱性检测	10
	1.4.3 流量探测	11
	1.4.4 报告中心	12
<u> </u>	登录	13
≡.	资产管理	14
	3.1 资产扫描	14
	3.1.1 扫描任务	14
	3.1.1.1 扫描任务一任务列表	14
	3.1.1.2 扫描任务新识别资产	16
	3.1.2 扫描结果	16
	3.1.3 区域配置	16
	3.2 资产预览	17
	3.2.1 资产台账	17
	3.2.2 资产测绘	18

	3.2.3	API 清单18
	3.3 其他	工具19
	3.3.1	设备端口扫描19
四.	脆弱性检测	
	4.1 脆弱	性检测包21
	4.1.1	基本配置21
	4.1.2	高级选项22
	4.2 任务	管理31
	4.2.1	任务列表31
	4.2.2	工作列表40
	4.3 数据)	库检查41
	4.3.1	检测基本配置41
	4.3.2	登录信息选择42
	4.3.3	存活配置选项43
	4.3.4	探测选项44
	4.3.5	检测选项44
	4.3.6	引擎选项45
	4.4 安全	基线检测46
	4.4.1	在线任务-检测基本配置46
	4.4.2	离线任务-检测基本配置49
	4.5 脆弱	性资产50
	4.5.1	系统资产51
	4.5.2	Web 资产54
	4.5.3	新增资产56
	4.5.4	删除资产57



	4.5.5 编辑资产57
	4.5.6 查询资产
	4.5.7 资产导出
	4.6 脆弱性资产组60
	4.6.1 新增资产组60
	4.6.2 删除资产组61
	4.6.3 新建基线策略62
	4.6.4 基线离线模板62
五.	脆弱性模板64
	5.1 基线策略模板64
	5.1.1 新建基线策略64
	5.1.2 基线离线模板65
	5.2 口令字典
	5.2.1 上传口令字典66
	5.3 WEB 插件67
	5.3.1 新增 Web 插件模板68
	5.4 系统插件69
	5.4.1 新增系统插件模板69
六.	流量探测71
	6.1 新建任务71
	6.1.1 新建任务71
	6.2 探测预览71
	6.2.1 探测预览71
七.	敏感探测
	7.1 数据库资产73



	7.1.1 数据库列表
	7.1.2 探测进度
	7.2 敏感数据发现75
八.	合规检查77
	8.1 法规合规检查77
	8.2 知识库
九.	报告中心79
	9.1 资产报告导出
	9.2 脆弱性导出
	9.2.1 输出报表
	9.2.2 报表列表
	9.2.3 报表详情
+.	系统配置98
	10.1 系统状态
	10.2 报告输出配置98
	10.3 出境填报99
	10.4 诊断工具100
	10.4.1 端口探测工具100
	10.4.2 Ping 工具 101
	10.4.3 Tcpdump 工具 101
	10.4.4 信息故障收集102
+-	Sysadmin 系统配置103
	11.1 系统状态
	11.2 漏扫 license 103
	11.3 网络属性104



11.4 IP 配置管理	
11.5 漏扫升级	
11.6 资产识别指纹	
11.7 一键清除	



前 言

内容简介

节章	概述
1.产品概述	介绍 DCBox 的背景、体系结构、部署方式、产品定位等信息。
2. 登录	介绍 DCBox 的登录的功能。
3. 典型策略配置案例	介绍 DCBox 的典型策略配置案例。
4. 资产管理	介绍 DCBox 的资产扫描、资产预览等的相关功能。
5. 脆弱性检测	介绍 DCBox 的系统扫描、WEB 扫描、弱口令扫描等的相关功能。
6. 脆弱性模板	介绍 DCBox 的基线策略模板等的相关功能。
7. 流量探测	介绍 DCBox 的流量探测等的相关功能。
8. 敏感探测	介绍 DCBox 的敏感探测等的相关功能。
9. 合规检查	介绍 DCBox 的法规合规检查、知识库等的相关功能。
10.报告中心	介绍 DCBox 的资产报告导出、脆弱性导出等的相关功能。
11. 脆弱性模板	介绍 DCBox 的基线策略模板等的相关功能。
12.系统配置	介绍 DCBox 的资系统监控等的相关功能。

获得帮助

文档意见反馈

可以通过以下方式反馈在文档使用过程中遇到的任何问题和对文档的建议和意见。

邮箱: service@seclead.cn

售后服务

提供全国范围内的服务热线,可以帮助用户解决在使用安全设备和服务过程中遇到的各种问题和困难。 服务热线 网站: https://www.seclead.cn 服务电话: 400-9919-700



一. 产品概述

本章主要内容如下:

功能	描述				
背景	简单介绍 DCBox 产品的背景。				
体系结构	介绍 DCBox 的体系结构。				
部署方式	介绍 DCBox 的部署方式。				
产品定位	介绍 DCBox 的主要功能。				

1.1 背景

当今数字化时代,随着各种网络应用的广泛应用和互联网技术的不断发展,网络空间已成为人们生活和工作的重要组成部分。与此同时,网络安全问题也日益突出,网络攻击、数据泄露等事件频频发生,并且近年来,漏洞数量也呈快速增长的趋势,长期处于严峻状态,给企业安全带来了巨大的挑战,另外,除了脆弱性漏洞之外,各种流量中的隐含风险也时时刻刻影响着企业单位的安全,如各种是恶意攻击风险,比如黑客可能通过篡改或模拟请求、进行 DDoS 攻击等方式,使得 API 服务出现故障、崩溃甚至被控制,从而对系统造成巨大损失。

随着《网络安全法》、《数据安全法》、《个人信息保护法》等法律文件的相继颁布, 各行业主管部门和地方政府也纷纷出台数据安全条例规范,国家开始进入数据安全强监管时 代。如何准确、快速地评估自身数据资产的安全状态,如何针对资产中的各种难以洞察的脆 弱性漏洞以及流量中的隐匿风险进行底数清,伴随着业务需求的产生,相应的解决方案也应 运而生。

市面上针对资产脆弱性及流量探测领域均有较为成熟的产品来覆盖需求,但总体而言, 能力集成较为分散,需要多种产品的组合,才能提供企业常规化的漏洞扫清与资产排查,为 企业提供更有效,更便捷的自查自检方法,亟需一款综合性便携式设备。

1.2 体系结构

羚见数据安全检查工具箱(DC-Box)系统是架构于自有的网络操作系统之上,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。





图 1.2 数据安全检查箱体系结构

▶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 部署方式

考虑到护网需求的常规化,DC-BOX 采用一体机式形态,即插即用,完全支持旁路部署在 核心交换机上,对各个区域的设备进行扫描,单机部署操作简单,且不改变客户现有网络结构。具体拓扑结构如图 1.3 所示。





图 1.3 部署方式

1.4 产品定位

1.4.1 资产管理

资产扫描功能为 DC-BOX 的核心能力之一,通过主动扫描的方式,全方位洞悉系统内的核 心资产,其中包括边界资产、web 资产、数据库资产、视频资产以及文件服务资产,并支持 手动注册添加至资产台账,联动地域等信息,一体化测绘出不同区域的资产全景,给管理者 提供有力的辅助决策支撑,实现资产全感知。当前资产管理模块主要有以下基本功能:

资产扫描:可实现对网络中的各类设备的扫描发现,可查看当前发现设备列表和历史发现情况,支持主动扫描探测等多种方式实现资产设备的发现。

区域配置与资产测绘:通过配置不同区域(省级,市级,区/县级,单位),形成区域字 典,自动联动已注册资产,自动化测绘出不同区域资产分布情况,并全方位展示于资产测绘;

资产台账: 实现对各类资产设备设备的信息维护、资产查询、和注册管理。可管理的资产包括边界资产、web 资产、数据库资产、视频资产以及文件服务资产等。

资产指纹识别:支持对设备类型的分析识别,通过检测设备操作系统、端口状态、设备 厂商等多种信息,可准确分析出设备类型。系统预置交换机设备、服务器设备、网络安全设 备、数据库服务器设备、边界交换设备等多种特征模型,支持设备类型分析模型的自定义配 量,可按照设备属性和运行参数等多种信息配量特征模型,包括设备端口、操作系统版本、 设备厂商等内容。

1.4.2 脆弱性检测

系统漏洞扫描: 主机系统上存储、处理和传输各种重要数据,一旦遭受攻击,将

可能导致程序运行失败、系统宕机、重新启动等后果,或者是获得主机上存储的敏感信息。更为严重的是,可以利用漏洞来执行非授权指令,甚至可以取得系统特权,从而控制整个主机,进而进行各种非法操作。

DC-BOX 支持针对网络环境中的各种主机、交换机路由器、防火墙、中间件等存在的常见漏洞、典型漏洞(如心脏出血)、0day 漏洞等进行扫描和检查。具体功能如下:

(1)支持扫描通用操作系统,涵盖 Windows 系列、苹果操作系统、Linux、AIX、HPUX、IRIX、BSD、Solaris 等。

(2)支持扫描交换路由设备,涵盖Cisco、Juniper、华为、F5、Checkpoint、锐捷在内的主流厂商的设备。

(3)支持扫描安全设备,涵盖 Checkpoint、赛门铁克、Cisco、Juniper、Palo Alto、 华为在内的主流厂商的防火墙等安全设备。

(4)支持扫描物联网设备,如主流厂商海康威视、宇视、华为、大华、Brickcom、索尼、 TP-LINK、AXIS、佳能等的摄像头,三星、惠普、爱普生、佳能等厂商的打印机。

(5) 支持针对工控专用设备包括 PLC、SCADA、DCS、工控专用网络设备的漏洞扫描。

(6)支持国产操作系统、数据库的扫描,国产操作系统包含中标麒麟、凝思、华为欧拉、 深度、红旗、中兴新支点,国产数据库包括神通、人大金仓、南大通用、达梦。

(7)支持大数据组件框架漏洞检测,如zookeeper、ElasticSearch、ActiveMQ、Kibana、 Hadoop 等。

Web 漏洞扫描: DC-BOX 提供广度和深度两种扫描方式,支持提供 OWASP 定义的 TOP 10 Web 威胁如注入(SQL 注入、Cookie 注入、Xpath 注入、代码注入、框架注入、Base64 注入、命 令注入、操作系统命令注入)、XSS 跨站脚本、伪造跨站点请求(CSRF)、网页挂马、暗链、 敏感信息泄露、安全配置错误等漏洞风险等漏洞扫描服务。通过基于爬虫的网站漏洞扫描技 术,能够有效识别 Web2.0 以及 Flash,保障 Web 漏洞扫描的全面性。进行网站结构分析、漏 洞分析,及时获得网站的漏洞情况,以及修补建议。



数据库漏洞扫描:采用先进的数据库发现技术和实例发现技术等,可针对当下主流的数据库,如 Oralce、MySQL、Postgres、IBMDB2、MongoDB、SQLServer、Informix、Sybase等进行漏洞检测,包括对数据库系统的各项设置、数据库系统软件本身已知漏洞、数据库系统完整性进行检查和对数据库系统的整体安全性做出评估,并给出提高数据库安全性的修复建议。通过登录扫描可对数据库的系统表甚至字段进行安全检测。

安全基线检测:安全配置核查是安全管理的基本工作,同时也是安全运维的重要技术手段。安全配置核查首先要建立满足组织信息安全管理体系的安全配置要求的基线。当前,部分重要行业和监管部门已经针对行业的信息系统建立详细的安全配置要求及规范。它构建针对不同系统的详细检查项清单和操作指导,为安全运维人员的安全技术操作提供标准化框架和指导,有很广泛的应用范围,主要包括新系统的上线安全检查、第三方入网安全检查、安全合规检查、日常安全检查等。

DC-BOX 参考国内外标准、行业技术规范和安全运维最佳实践构建了以业务系统为核心, 覆盖业务层、系统支撑层的安全配置基线模型。从业务系统安全要求出发,将要求分解到对 应的支撑系统的具体安全要求。支撑系统包括操作系统、数据库、中间件和应用系统,还包 括网络设备和安全设备等。针对这些支撑系统的具体产品类型如Windows,Oracle,Weblogic, 交换机,防火墙等,根据具体的安全要求可细化到可执行和实现的具体要求,并可以对同类设 备,不同品牌型号,形成具体的安全要求及配置检查方法。

弱口令扫描:对系统存在的弱口令做检测,支持知名的协议、数据库、中间件、

HTTP 服务、HTTPS 服务和摄像头检测如 TELNET、FTP、SSH、POP3、RDP、SMTP、Oracle、 MySQL、PostgreSQL、MsSQL、Sybase、Informix、HTTP、大华摄像头、华为摄像头等。系统 内置默认的字典库,并支持上传自定义的字典库,丰富平台弱密码检测能力。

1.4.3 流量探测

流量探测模块旨在于利用先进的技术和算法,实时捕获和解析网络中的 API 流量。通过 深入分析和监控 API 请求和响应,帮助用户全面了解其流量片段内的 API 使用情况以及对应 安全行为分析,以下是该功能的主要特点和优势:

实时监测和分析:无论是内部系统之间还是与外部第三方服务的交互。可以实时查看 API 请求和响应的详细信息,包括参数、状态码、返回结果等,便于快速定位和解决潜在的问题。

11

安全性评估:通过对 API 流量的深入分析,该产品能够评估 API 的安全性,并发现潜在的风险和漏洞。它可以识别出现的异常行为,并进行展示,将恶意行为以及潜在的安全威胁 实现底数清,帮助用户及时采取预防和修复措施,保护 API 和敏感数据的安全。

报告导出与共享:用户可以根据需要将 API 流量监测和分析的结果导出为报告,方便内部团队评估和决策。此外,用户还可以选择共享报告给相关的合作伙伴和第三方,以加强沟通和合作,并共同提升 API 的质量和安全性。

总之, API 流量探测功能能够为用户提供全面的 API 监测、安全性评估和不安全内容溯源, 并提供相关详细报告的导出,这将帮助用户及时发现和解决流量中的相关隐匿风险,确保了 系统的稳定性、安全性、保密性和完整性。



图 1.4.3 流量探测

1.4.4 报告中心

DC-BOX 支持资产台账、脆弱性全览以及流量探测预览的多种报告生成,并支持自选维度, 自定义的报告生成,包括报告名称、报告组件、可视化模块、及文字编辑等多样式,且支持 报告的预览与导出。

资产台账报告:统计资产数量,设备分类,资产类型等全方位的资产信息并整理汇总, 支持自定义分析与编辑;

脆弱性漏洞报告:统计漏洞数量、整改数量和整改率等各项数据,对数据进行报表化, 定期完成对所管辖资产的漏洞关联,形成漏洞统计报告;

流量探测预览报告:统计 API 流量探测的所有安全行为与不安全行为,并根据 API 模型 分类展示不安全行为的详细内容,便于分析与溯源。



笔记本电脑配置 192.168.0.X/24 的 IP 地址,并直连到 DCBOX 设备管理接口,默认为 MGT 或 ETHO 接口。打开浏览器(推荐谷歌或火狐浏览器),输入 https://192.168.0.52 访问数据 安全检查工具箱.登录首页面



图2登录



三. 资产管理

3.1 资产扫描

3.1.1 扫描任务

3.1.1.1 扫描任务---任务列表

任务列表分为待扫描、扫描中、已完成页面。

待扫描页面可进行新建任务、编辑、删除、开始扫描、批量删除等操作。

◎ 资产管理	◎脆弱性检测	☑ 脆弱性模板	し 流量探測	☑ 报告中心	田 系统配置					
◎ 资产管理 / Ⅰ 资产扫描 / 會扫描任务										
任务列表 + 新建任务 D 开始扫描 ① 批量删除 待扫描 扫描中 已完成										
序号		任务名		IP/文件	#名称	任务创建时间	状态	操作		
□ 1		test		[*172.2	0.54.100"] ~ ["172.20.54.19	2023-06-25 14:45:21	未扫锚	开始扫描 編輯 删除		

图 3.1.1.1-1 待扫描页面

WEBUI: 主界面 -> 资产扫描 -> 扫描任务 -> 新建任务

新建任务页面可进行扫描方式、资产类型的选择,还可进行白名单的设置。

新增任务		×
* 任务名称 任务名称		
扫描方式 手动单次		V
*资产类型 边界资产 视频资产	产 数据库资产 文件服务资产 WEB资产 其他	
API探测 关闭 开启]	
扫描IP段		+ 添加 上下载模板 上批量导入
序号 开始IP	结束IP	操作
	室无数据	
日描白名单		
【格式: 192.168.1.1-10,192.168.2.5.1	192.168.2.6-10,192.168.2.9]	1
		取消 确定





新建任务参数说明如表 3.1.1.1-1 所示:

表 3.1.1.1-1 参数说明

参数	说明
任务名称	资产扫描任务的名称
扫描方式	资产扫描定时方式;分别为手动单次、即时单次、每30分钟、每小时、每天、每周、 每月、每3个月、每6个月、每年
资产类型	扫描的资产类型:可选项分别为边界资产、视频资产、数据库资产、文件服务资产、WEB 资产
API 探测	API 探测关闭,不进行 api 资产的扫描, API 探测开启,进行 api 资产的扫描,包括 http 与 https 的资产
任务列表	可填入开始 IP: 192.168.0.1 结束 IP: 192.168.0.255
扫描白名单	可填入 IP/IP 范围,扫描时跳过该 IP/IP 范围的资产,不进行该资产的扫描

扫描中的页面可停止扫描。

②资产	管理	◎ 脆弱性检测	☑ 脆弱性模板	し 流量探測	🖸 报告中心	田 系统配置					
◎ 资产管理	◎ 资产管理 / Ⅰ 资产扫描 / 會扫描任务										
任务列 待扫描	岐	扫描中	己完成								+ 新建任务 口开始扫描
	序号	任务名称	IP/文	牛名称	开始时间	状态	端口扫描进度		http扫描进度	扫描次数	操作
	1	任务名1	["172.	20.0.0"] ~ ["172.20	2023-06-25 14	4:49:15 扫描中	I			570次	停止扫描

图 3.1.1.1-3 扫描中页面

已完成页面可进行新建任务、批量删除、删除、重扫、查看、下载等操作。

◎资产	管理	◎ 脆弱性检测 ◎ 脆弱性模板	□ 流量探测 □ 报告中心	田 系統配置						
⊙ 资产管理	◎ 资产管理 / I 资产扫描 / 會扫描任务									
日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日	康	扫描中 已完成						+ 新建任务 自 批量删除		
	序号	任务名称	IP/文件名称	开始时间	结束时间	扫描次数	状态	操作		
	1	任务名1	["127.0.0.1"] ~ ["127.0.0.1"]	2023-06-25 14:48:40	2023-06-25 14:48:45	2次	扫描完成	删除 重扫 查看 下载		
	2	任务名1	["172.20.0.0"] ~ ["172.20.255.255"]	2023-06-25 14:49:15	2023-06-25 14:50:56	571次	已停止	删除 重扫 查看 下载		
	3	任务名1	["172.20.0.0"] ~ ["172.20.0.255"]	2023-06-25 04:05:34	2023-06-25 04:07:19	12次	扫描完成	删除 重扫 查若 下载		
	4	copy-任务名1	["172.20.0.0"] ~ ["172.20.0.255"]	2023-06-05 14:07:38	2023-06-05 14:09:28		扫描完成	删除 重扫 查看 下载		
	5	NICE	["172.20.57.51"] ~ ["172.20.57.51"]	2023-06-05 13:48:38	2023-06-05 13:48:43		扫描完成	删除 重扫 查看 下载		
	6	FDSFS	["199.11.1.1"] ~ ["199.11.1.1"]	2023-06-05 14:34:48	2023-06-05 14:34:53		扫描完成	删除 重扫 查看 下载		
	7	172.20.57.12	["172.20.57.12"] ~ ["172.20.57.12"]	2023-06-05 19:15:33	2023-06-05 19:15:38		扫描完成	删除 重扫 查看 下载		
	8	新建的任务0606	["172.20.54.100"] ~ ["172.20.54.1	2023-06-11 16:09:14	2023-06-11 16:09:54		扫描完成	删除 重扫 查看 下载		
	9	TEST	["172.20.57.51"] ~ ["172.20.57.51"]	2023-06-06 13:52:34	2023-06-06 13:52:39		扫描完成	删除 重扫 查若 下载		
	10	172.20	["172.20.54.1","172.20.52.1"] ~ ["	2023-06-06 19:05:09	2023-06-06 19:05:16		扫描完成	删除 重扫 查看 下载		
							< 1	2 3 4 5 6 >		

图 3.1.1.1-4 已完成页面



3.1.1.2 扫描任务--新识别资产

新识别资产展示扫描任务中新发现的资产列表,可进行添加、删除、批量添加、批量删除等操作。添加后的资产在资产预览-资产台账处展示,资产来源为扫描。

								and the second second	and the state
任务名称	IPUEL	资产类型	总中URL	命中就口	Γ R	API存活数	开放端口	发现时间	操作
test1031	172.20.54.206	文件服务遗产	220	21	FTP	0	21.111.2181	2023-10-31 10:39:22	添加量統
test1031	172.20.54.210	WEB 把P	https://172.20.54.210:443/		19:90	0	22.111.3306.8000.443.6379.80.2505	2023-10-31 10:39:28	20.00 新統
test1031	172.20.54.231	WEB资P	http://172.20.54.231:80/		***	0	22.3306,6379,80.8080,9999,8081	2023-10-31 10:39:46	STATE BEAR
test1031	172.20.54.236	WEB 进产	http://172.20.54.236:8080/		未知	0	111.3306.443.9090.80.9060.2181	2023-10-31 10:39:52	iāna Bibl
test1031	172.20.54.237	WEB资/**	https://172.20.54.237:443/		#30	0	10080.8080,2181,10008,111,3306,443,9090,80,10000,10010,10002,10024,10001,10012,10003,10025	2023-10-31 10:39:58	15.00 B186
test1031	172.20.54.240	WEB避₽#	https://172.20.54.240:443/		未知	0	22.111.3306.8000.443.6379.80.2505	2023-10-31 10:40:04	添加 副版
test1031	172.20.54.244	WEB资产	https://172.20.54.244:443/	2227	沖加	0	22.111.3306.8000.443.6379.80.2505	2023-10-31 10:40:10	15.70 BIN
test1031	172.20.54.248	数据库资产	770	2181	Zookeeper	0	111.2181.9999.59200.59999	2023-10-31 10:40:22	15.00 Bills
test1031	172.20.54.251	其他			(777)	0	22	2023-10-31 10:40:25	添加 動動
test1031	172.20.54.252	其他	****			0	22	2023-10-31 10:40:28	运动 删除

图 3.1.1.2-1 新识别资产列表

3.1.2 扫描结果

扫描结果展示已扫描出的资产,扫描结果列表展示注册过及未注册的资产,可进行添加、删除、批量添加、批量删除、导出发现列表等操作;支持资产类型、厂商名称、IP地址、设备分类、是否注册、区域 名称的查询。

扫描结果分为常规列表、探索列表,对边界、web、数据库资产指纹进行分类与二次验证,提升资产 扫描精准度。

199		◎ 资产管理	⊙ BERTHERENN		IN SERIER		□ 報告中心	© SIGNE									
的目標	^	◎ 流产管理 /	工资产扫描 / 🖸 扫	原结果													
12 扫描任务		资产类型	资产关键			v .	厂商名称 7	南名称				IPHENE IPHENE				へ 重日	CE
11倍结果		设备分类	0294			0	暴而注册	1511.0			~	KHAR Esta					
15.14623B																	
o預認		扫描结果												- L	9312630968 + #2#	t ntāt	① 北景田
:IЩ	÷	常规列表	经期利期												?*		
		0.4	19	Г. <mark>В</mark>	资产类型	IPIELE	ARRIST	是古新发现	开放端口	命中URL	命中編日	APIFyi38	设备分类	是否注册	发现时间	an	
		0.1		杭州颂信	边界资产	172.20.57.138		香	22,111,3306.8000.44	https://172.20.57.13		4	视频交换平台	已注册	2024-05-07 17:31:46	90bb	
		2		杭州硕信	边界资产	172.20.57.139		8	22,111,3306,8000,44	https://172.20.57.13	100 C	4	视频交换平台	已注册	2024-05-07 17:31:45	Bills	
		0 3		杭州领信	边界资产	172.20.57.177	220	Ħ	443.80	https://172.20.57.17	223	2	MB	已注册	2024-05-07 17:31:44	肥味	
				杭州硕图	WEB (80)PP	172.20.57.179		M	22.59999.111.443.80	https://172.20.57.17		6	RS	日注册	2024-05-07 17:31:45	Bith	
				杭州顿信	WEB 300	172.20.57.183			111,3306,443,9090,8	https://172.20.57.18	4440.0	6	MB	已注册	2024-05-07 17:31:45	B10	
		0 6		杭州硕信	WEBBEPM	172.20.57.184		8	3306.443.80.2181	https://172.20.57.18		3	其他	已注册	2024-05-07 17:31:45	副助	
		0.7		杭州顿德	WEB(E)#	172.20.57.197		60	22,59999,111,443,80	https://172.20.57.19_		6	其也	已注册	2024-05-07 17:31:46	Bits.	
		8		杭州绥信	WE8进产	172.20.57.241		晋	443.80	https://172.20.57.24		λ	NG	已注册	2024-05-07 17:31:46	Bilth	
		9		VMware	WEB(85)**	172.20.57.251		폽	8000.443.9080.80	https://172.20.57.25	100	3	#S	已注册	2024-05-07 17:31:46	删除	
		0.1	0	机州总信	WEB 例件	172.20.57.51		百	22,59999.111,443,80	https://172.20.57.51:	***	7	×s	已注册	2024-05-07 17:31:46	劉統	
														共计34条 <	1 2 3 4	> 1	10 条/页

图 3.1.2 扫描结果

3.1.3 区域配置

区域配置把对应资产与相关区域对应起来,方便"资产测绘"页面的展示,点击"新增"按钮,弹出 新增配置的页面,配置区域为必填项。



⊙ 资产管理	◎ 脆弱性检测	量探測 🛛 报告中心 🖽 系	统配置			
◎资产管理 / 工	资产扫描 / 🗈 区域配置					
IP地址范围	IP地址范围	区域名称 区域名称		时间	开始日期 ~ 结束日期	白 Q 査询 C 重置
区域配置						+ 新増
序号	IP地址范围	区域名称	区域等级	相关单位	更新时间	操作
1		上海市/上海市/黄浦区	区/县级		2023-06-08 17:00:03	编辑 删除
2	172.20.57.51-172.20.57.52	内蒙古自治区	省级		2023-06-11 17:19:04	編辑 删除
3		内蒙古自治区/呼和浩特市/新	区/县级		2023-06-08 16:59:25	编辑 删除
4		北京市	省级		2023-06-08 16:17:02	编辑删除
5	255.255.255.1	北京市	省级	9090	2023-06-08 16:16:40	编辑 删除
6		吉林省/长春市/南关区	区/县级		2023-06-08 16:59:43	编辑 删除
7		天津市/天津市/南开区	区/县级	公安局	2023-06-07 19:41:32	编辑 删除
8	255.255.255.1	天津市/天津市/和平区	区/县级	和平	2023-06-07 19:41:35	编辑删除
9		天津市/天津市/河东区	区/县级		2023-06-08 16:58:34	编辑 删除
10	127.0.0.1	天津市/天津市/河西区	区/县级	公安局9	2023-06-11 14:53:54	编辑 删除
						< 1 2 3 4 >

图 3.1.3 区域配置

3.2 资产预览

3.2.1 资产台账

资产台账展示已注册的资产列表,分级展示区域配置中新增的配置级别。支持区域、资产名称、资产 类型、设备分类、资产 IP 地址查询。支持列表导出操作。

🕐 数据安全检查	工具箱系统															
8	◎焼产管理				0 10017785	⊙ А <u>яйа</u> ⊡ I	1940 8 1667									
工 建产扫描 🗸	◎ 洪严管限 / 日	1 100°5000 / 100	资产台张													
□ 資产預点 ▲	wgs	NUM														
洲 资产台账	市委	新加速														
< 资产制度	IX BUB	UNIT 12														
凸 API通举	EMM/2	all contraints														
e mein .	BIX BILL	DEMONTS.														
	资产名称	B#6R				资产集	aras a			×	设备分类	-			~	9. 159 C 188
	资产IP地址	把户印始起				徵产臣	10750 B			v	资产来源	jer na			v	
	▽ 检察结果														+ 1630	と母出しの出意時神
		#9	资产名称	资产类型	设备分类	IPIEb2/IEE	资产包属	资产医线	FINAL	ГА	2 9		资产来源	生产日期	是否过保	B ft
		1	test1030	発信	1.66	172.20.53.132	浙江省/杭州市/演江				100		1338			REMARCE WALL BODS
		2	123	WEBER-	減位	172.20.53.181	浙江省/杭州市/滨江	9 4 12	8080				1318			
		3	asdasd1112	WEBSE	其他	172.20.54.167	浙江省/杭州市/演江	5	111.443.80.2505	65/HI05/W	1773		相關	100		
		4	asdasd1111	WEBBO	34.65	172.20.54.17	浙江省/杭州市/高江	生产区	111,443,00,2505	杭州资源			1052			REMARCE WAR BARE
		5	172.20.54.36	WE8證产	VPN	172.20.54.36	浙江省/杭州市/滨江	±#E	111.10000				1016	+++		
		6	12354.54的图产名称	边界进产	#10/0#	172.20.54.54	近日第4批州市/港口						手动			LENDINGLIC HANNE BURG
			172.20.54.225mysql	数据库资产	興也	172.20.54.225	浙江南/杭州市/演江		80.111		100		手的	***		
			172.20.54.135回形数。	数据库资产		172.20.54.135	派江南/杭州市/南江				-		手动	+++		刷新编口 编辑 静脉
		9	172,20.52.135TIDB	的想向日产	1.772	172,20,52,135	浙江省/杭州市/清江	2		1.000			于动			
		10	172.20.54.20毫新100	数据库资产	MIS	172.20.54.20	IEI第/RHR/RI		80				手讷			

图 3.2.1 资产台账

点击"新增",展示新增资产相关弹窗,有17个输入项,其中资产名称、资产类型、资产归属、资产 IP 为必填项。



所增资产							
资产名称	请输入资产名称	* 资产3	建型 请输入资产类型	v	*资产归属	请输入资产归属	
设备分类	请输入设备分类	∨ 部署[【岐 请输入部署区域	v	MAC地址	请输入MAC地址	
*资产IP	请输入资产IP	厂商名	3称 请输入厂商名称		机柜位置	请输入机柜位置	
操作系统	请输入操作系统	维保全	F限 请输入维保年限		资产型号	请输入资产型号	
生产日期	请输入生产日期	白 责任	EL 请输入责任人		管理地址	请输入管理地址	
主管单位	请输入主管单位	联系力	方式 请输入联系方式				

图 3.2.2.1 新增资产

3.2.2 资产测绘

资产测绘可视化展示所有已注册资产的区域归属情况及不同区域资产的分布情况。左上可进行区域筛选,每个区域右上角均有+按钮,点击将从下方出现相关区域的资产概况,右侧可进行资产展示的放大、缩小、自适应、全屏、退出全屏、切换布局、全选节点、取消全选操作。

			0 1000 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0					
) 激产扫描	*	◎ 治疗管理 / □ 治疗规范 / ≤ 治疗理論						
资产预点	•	一日设备	类型分布				1 厂商分布	
H 资产台账			WEB#77				70-	
< RAM8		-	文件服务资产		● 边界街	≓: 1	60	
(S APUBR		(iii)			• संद्रावाल	PF: 1	50	
MEIN		 - 已注册:72 - 未注册:56 			 数据等 文件部 	资产:21 务资产:1	40	
		发现设备	- RS80+70		• WEBB	0≊: 15	20	
		69台	20044		• 発位:	33	10	-
			边界进产				#10 11111 PR	大州新信
		0.00. 05/7.04						10
		2.12 (11) (11) (11)			WIN	+		-
				Noff*		39		Т
								6
								4
				10.000	60104	+		
				ec.ar-				
					×IE	+		
				BORT		39		
					领信数科	+		
				NOS.		39		

图 3.2.2 资产测绘

3.2.3 API 清单

API 清单展示资产扫描与流量探测处扫描出的 API 资产列表,可进行资产名称、资产分类、API 来源的筛选操作。

点击"添加",可手动添加 API 清单列表。



添加API		X
* IP地址	请输入IP地址	
* URL	请输入URL	4
		取消 确定

图 3.2.3-1 添加 API

API 清单展示手动添加、资产扫描、流量探测来源的数据。

12	○ 资产管理	⊙ BERTHERENN EI BERTHEREN	RE IN TEREFRON 📿 RECON	738 ○台東絵査 □報告中心 章	SARE			
た 日福 ・	◎ 田产管理 / 国	田市知道 / ⑤ API春曲						
体模型 A	资产名称	MAXB#68		资产类型 新加入资产类型	 APIR語 浙沧入AP 	(4)资	v	く、鹿田
一 资产别给	APISO							15 tn 2
) API酒单	1 A. 1414	资产名称	IP增量/服务	资产类型	URL	API来源	题件	
) 风险资产管理	1	172.20.57.1	172.20.57.1	WEB(何) ⁴⁴	http://172.20.57.1:8080/https:/172.20.5	资产扫描	SALE BILL	
reių .	2	172.20.57.1	172.20.57.1	WEB ##	http://172.20.57.1:8081	资产扫描	SALA BUD	
	3	172.20.57.29	172.20.57.29	数据库资产	http://172.20.57.29/8082	谢产扫描	SALE BID:	
	4	172.20.57.29	172.20.57.29	数据库资产	http://172.20.57.29:8088	资产扫描	9418 1939:	
	5	172.20.57.29	172.20.57.29	数据库资产	https://172.20.57.29.8088	资产扫描	编辑 删除	
	6	172.20.57.29	172.20.57.29	数据库资产	https://172.20.57.29/8082	资产扫描	94412 1932	
	7	172.20.57.214	172.20.57.214	純 他	http://172.20.57.214:9090/	资产扫描		
	8	172.20.57.214	172.20.57.214	MAL	https://172.20.57.214:9090	资产13届	will blick	
	9	172.20.57.214	172.20.57.214	34 /B	http://172.20.57.214:8083	资产扫描	9418 2019:	
	10	172.20.57.214	172.20.57.214	將位	http://172.20.57.214:8061/	资产扫描	Sata Bith	
								共计375条 < 1 2 5 4 5 38 > 10家

图 3.2.3-2 API 清单

点击"列表导出",导出当前列表的 API 清单数据。

3.3 其他工具

3.3.1 设备端口扫描

设备端口扫描可通过 ip 地址检索并查看相关的设备启用的端口,支持设备端口导出。





Name Constraint Constraint Constraint Constraint Seriescone Press Press Press Press Seriescone V dedag MCD6 /// ML MCD6 /// ML <th></th>	
Composition Composition <thcomposition< th=""> <thcomposition< th=""></thcomposition<></thcomposition<>	
NUMBER V 1604R LUC9:22 LUC9:11 LUC9:24 LUC9:256 LUC9:256 LUC9:256 LUC9:105 LUC9:110 LUC9:110 LUC9:256 LUC9:106	F2
C D	r: 7
EEStell on EEStell part EEStell part <th>48(1)20-900A</th>	48(1)20-900A
Image: constraint of the	IEEE TANK
B CTUE SPCIE Vertil SPCIE Herb, SPCIE HER	F 4
READ prime READ prime <thread prim<="" th=""> READ prim READ prim<</thread>	MC1451 38788
ի պի պի պի պես մե մե մե մե մե մե	股所有称 uninown
10(0):0108 80(0):5179 80(0):5199	L
BARD months BARD months	
Bibliote markets Bibliote Markets Bibliote Markets	

图 3.3.1 设备端口扫描



四. 脆弱性检测

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

4.1 脆弱性检测包

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,对漏洞扫描结果有相应的描述、解决方法和检测详细。

4.1.1 基本配置

WEBUI: 主界面 -> 脆弱性检测 -> 脆弱性检测包 -> 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,仅存活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。

□ 新建任务			
基本配置 高级选项			
新建任务类型	✔ 系统扫描 Web扫描	□令猜解 (存活探测)	*提示:如勾选仅存活探测,则不进行漏洞扫描,仅探测资产存活状态和满口开放情况
扫描目标方式	● 手动输入 ○ 使用资产	○ 批量导入	
扫描目标			* 扫描目标填写规范: IP4本示例192.168.1.100,IPv6示例: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
任务名称			*提示:请填写任务名称,长度在[1-40]字符之间
执行方式	立即执行	*提示: 请选择执行方式	
系统漏洞模板	全部漏洞扫描	* 提示: 请选择漏洞插件模板	
检测模式	标准扫描	标准扫描: 默认选择标准端口的端口范围, 采用主机存;	活判断、端口扫描、服务判断、漏洞测试的步骤对扫描目标进行完整的安全扫描 *****
		完全扫描: 民运的外门相口标运门工作作用, 调口成为 完全扫描: 默认选择全部端口的端口范围, 采用主机存 深度扫描: 利用配置好的用户名密码列表对主机进行登	⁷⁶⁰⁰ 活判断、靖口扫描、服务判断、漏洞则试的步骤对扫描目标进行完整的安全扫描 录后的安全扫描
调试模式	×	若开启,则记录目标详细插件执行日志。	
执行优先级别	÷. •	*提示:当任务达到并发上限时, '排队等待中'级别高的任	迁务将优先执行
分布式引擎	默认 *	* 默认:系统将根据引擎的负载情况,智能选择工作引擎 *注意:下发口令猜解任务若使用非默认字典,系统将自	[local: 系统将会选择本地号] 擊 动选择本地默认引擎
告警模板	无	*提示:告警发送配置,请到[系统管理>任务告警]下设置	Ē
	提交		

图 4.1.1 基本配置

基本配置参数说明如表 4.1.1 所示:

表 4.1.1 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,仅存活探测,如勾选仅存活探测,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: 1. IP 示例: 192.168.1.100,2001:fecd:ba23:cd1f:dcb1:1010:9234:4088 2. 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.* 3.域名示例: www.example.com 4. URL 示例: http://192.168.1.100/,https://www.example.com/,http://[2001:fecd:ba23:cd1f :dcb1:1010:9234:4088]/ 5. 排除某个 IP: 192.168.1.0/24!192.168.1.100						
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 7 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 3 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 36 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						
检测棋式	无:选择仅做存活探测的时候,没有展示						
1997次十八	可自定义扫描模式: 1. 标准扫描:默认选择标准端口的端口范围,采用主机存活判断、端口 2. 扫描、服务 判断、漏洞测试的步骤对扫描目标进行完整的安全扫描。 3. 快速扫描:快速的对扫描目标进行主机存活、端口服务探测。 4. 完全扫描:默认选择全部端口的端口范围,采用主机存活判断、端口扫描、服务判断、漏洞测试的步骤对扫描目标进行完整的安全扫描。 5. 深度扫描:利用配置好的用户名密码列表对主机进行登录后的安全扫描。						
调试模式	默认不记录扫描执行日志,若开启将记录扫描执行日志。						
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						

4.1.2 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。

會 系统监控									
 · · ·	日 新建住	1务							
新建任务	基本配置	高级选项							
□ 任务管理	系统扫描 WEB扫描	登录信息选项 探测选项						新增+ 批加	验证 2 刷新
◎ 数据库检测	口令猜解	检测选项	目标地址	服务	端口	用户名	密码	操作	验证结果
② 安全基线检测	存活探测	引擎选项	没有检索到数据						
103 资产管理		其它配置							< >
壹 资产组管理									
三 导出报表									
☑ 模板管理									
资产对比 *									
③ 系统管理 *									

图 4.1.2 高级选项

4.1.2.1 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

會 系统监控	□ 新建	任务							
 ○ 脆弱性管理 ✓ ✓ 新建任务 	基本配置	高级选项							
口 任务管理	系統扫描 WEB扫描	登录信息选项探测选项						新增+ 批調	建造证 2 刷新
② 数据库检测	口令猜解	检测选项	目标地址	服务	端口	用户名	密码	操作	验证结果
② 安全基线检测	存活探测	引擎选项	没有检索到数据						
103 资产管理		其它配置							< >
壹 资产组管理									
亘 导出报表									
③ 模板管理									
资产对比									
) 系统管理									

图 4.1.2.1-1 系统扫描-登录验证

登录验证配置参数说明如表 4.1.2.1-1 所示:

表 4.1.2.1-1 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

4.1.2.2 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。



□ 新建任	务			
基本配置	高级选项			
系统扫描	登录信息选项			
WEB扫描	探测选项	提示被扫目标	×	在扫描之前提示被扫描主机,需要扫描目标支持messager服务
口令猜解	检测选项			
存活探测	引擎选项			
	其它配置			

图 4.1.2.2-1 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

4.1.2.3 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。

⊖ 新建任	务		
基本配置	高级选项		
系统扫描	登录信息选项		
WEB扫描	探测选项	最大限度报告漏洞	✓ 若选择开启:扫描结果中不是所有漏洞都经过原理扫描得出,会有一些根据版本信息推测出来的漏洞
口令猜解	检测选项	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
存活探测	引擎选项	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,因此填用
	其它配置	启用口令破解	✓ 使用默认字典对系统或服务的□令进行猜解
		测试Oracle账号	×
		扫描模式	● 全面优先 ○ 准确优先

图 4.1.2.3-1 系统扫描-检测选项

检测选项配置参数说明如表 4.1.2.3-1 所示

表 4.1.2.3-1 酉	己置参数说明
---------------	--------

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
执行依赖插件	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



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

4.1.2.4 系统扫描---引擎选项

⊖ 新建任	务				
基本配置	高级选项				
系统扫描	登录信息选项				
WEB扫描	探测洗顶	插件超时(秒)	30	\$	单个插件执行时间最长设置[10-300]
		单个主机检测并发数	5	0	针对单个的检测目标,并发的检测插件数量[1-50]
니국에까	和空观地理以				
存活探测	引擎选项	单个扫描任务并发主机数	500	<u></u>	单个扫描任务,可同时扫描的王机数量[1-500]
	其它配置	单个主机TCP连接数	45	\$	针对单个检测目标,并发的TCP连接数量[1-1024]

图 4.1.2.4-1 系统扫描-引擎选项

引擎选项配置参数说明如表 4.1.2.4-1 所示:

表 4.1.2.4-1 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]

4.1.2.5 系统扫描---其他配置



基本配置	高级选项			
统扫描	登录信息选项			
/EB扫描	探测选项	微软WSUS地址		
令猜解	检测选项	微软WSUS端口		
活探测	引擎选项	微软WSUS账号		
	其它配置	微软WSUS密码		
		使用https	×	

图 4.1.2.5-1 系统扫描-其他配置

4.1.2.6 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

⊖ 新建任	务			
基本配置	高级选项			
系统扫描	登录扫描			
WEB扫描	引擎选项	起始URL		
口令猜解	检测选项	其他URL		
存活探测		网站域名		
		扫描根目录		
		例外URL		
		登录认证	无	The second secon
		上传网站证书	选择文件】未选择任何文件	浏览器客户端证书,如PFX/PKCS12等格式
		上传网站证书密码		导出证书时设置的密码

图 4.1.2.6-1 Web 扫描-登陆扫描

4.1.2.7 WEB 扫描---引擎配置

□ 新建任	务									
基本配置	高级选项									
系统扫描 登步 WEB扫描 引調 口令猜解 检验 存活探测	登录扫描 引擎选项 检测选项	并发送程数 区分大小写 最大类似页面数 回日录下最大而而数	5 () 20 () 100 ()	单个扫描目标,并发执行的线程数量[1-50] 网站对于Url中字母大小写是否敏感 引擎用于归并类似链接时需要使留类似链接的数量[1-1000] 引擎在旧并转换时,同一日带下需要保留处链接数量[1-1024]						
		重试次数 超时时间(秒) 单个网站扫描超时设置 代理类型	30 30 元	当結婚无法访问时,重新访问的次数(1-10) 当访问結婚的超过多长时间,判定结婚无法访问[1-300] 默认:0无限制,单位:小时 ▼ 网络访问目标网站时,可能需要通过代理才能访问 课句:1//理告标题:3.1元,查示则会目标/2.5元号目标						
		静态host配置		周期37月20日 引擎对场给的邮料,多个城会到P的对应关系以多大证号()。或换行分隔 城客与P的对应使式示例,www.example.com 192.168.1.0 类似192.168.3.cc、192.168.bb.cc、192.aa.bb.cc格式将会被视为域名。请确认后提交						

图 4.1.2.7-1 Web 扫描-引擎配置

Web 扫描-引擎配置配置参数说明如表 4.1.2.7-1 所示:

表 4.1.2.7-1 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]
单个网站扫描超时设置	默认:0 无限制,单位:小时
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
静态 host 配置	引擎对域名的解析,多个域名与 IP 的对应关系以英文逗号(,)或换行分隔 域名与 IP 的对应格式示例: www.example.com 192.168.1.0 类似 192.168.3.cc、192.168.bb.cc、192.aa.bb.cc 格式将会被视为域名,请 确认后提交

4.1.2.8 WEB 扫描--检测选项

本配置	高级选项				
统扫描	登录扫描				
EB扫描	引擎选项	暗链检测	×	发现网站中的存在的其他隐藏链接	
令猜解	检测选项	网站木马检测	× .	检测网站中是否存在恶意脚本	
活探测		检测深度	5	检测网站时爬虫爬取网站的页面深度[1-50]	
		爬虫策略	广度优先	v	引擎的爬虫在爬取网站页面多叉树时,采用的先后顺序策略
		HTTP请求头	Mozilla/5.0 compatib	ole; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0	引擎爬虫模拟浏览器的UserAgent
		表单填充内容	1		引擎爬虫模拟提交时需要填充的表单的内容
		最大页面数	5000	引擎爬虫爬取页面时超过最大页面数后,不做爬取	[1-10000]
		页面最大KB数	5120	引擎爬虫爬取页面时,如果页面大小超过一定大小	,则放弃爬取[1-102400]
		例外URL	logout.,sigout.,exit.		引擎爬虫不爬取的url关键字,一般为登出页面、危险操作、或不想做检测的链接
		例外操作按钮	×	引擎爬虫不触发带有关罐字的按钮,如删除、关机	、恢复出厂等,未开启时,无二次确认的按钮会直接触发按钮效果
		例外文件类型	.rar,.wmv,.doc,.docx,.a	avi,.rmvb,.asf.asx,.mid,.bin,.cab,.exe,.ico,.mdb,.mov,.mp3,.mp4,.	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	ASP.NET SessionID,A	SPSESSIONID, PHPSESSID, SITESERVER, sessid, VIEWSTATE, V	引擎对默认的参数不做安全检测

图 4.1.2.8-1 Web 扫描-检测选项

Web 扫描-检测选项配置参数说明如表 4.1.2.8-1 所示:

表 4.1.2.8-1 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

4.1.2.9 口令猜解---字典选择

2							
新校 道22		Glassman	· 住台橋元	* GlassFahs世俗于用		04L1 4545	e tres
藏物性被摄 ^	HTTP服务类型	http-get	6985	• http-geti8余字典		180 m	3283 o
13 新使任何			urt /admin/togin.asp			http-get请求页至un	
		http-get-form	(1) 使用于 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	* http-get-form语合字典		ca Ellet	艇时 0
			url /admin/login.asp			http-get-form请求页面url	
O DRAWER			data usemame=^USER^&password=^PAS	S ⁿ		注意: ^USER ^和 ^ PASS * 为字曲出位符号、禁止信号	zi
③ 安全基格检测			成沈明拉 - success			地区内容中包全的关键字	
15 東产管理		http-post-form	協会構成	* http-post-formag会字曲	*	1月日 80	逆时 0
≥ 奥产蜡糖器			utf /admin/login.asp			http-post-form请求负置url	
ⅲ 导出探表			data usemame=^USER^&password=^PAS	5 ⁿ .		注意: ^USER^和^PASS^为字典占位符号,禁止续召	81
40xice(# -			成功调度 - success			病型内容中包全的关键字	
9 月秋社 -		http-head	级白银式	* http-head協会字典	*	00 E3RE	照时 0
EGME -			url /admin/login.asp			http-head请求页面url	
			clista usemame=^USER^&password=^PAS	5 n		注意: ^USER ^和 ^PASS ^为字曲占位符号,禁止惊召	E1
			成功响应 - success			或亞內容中检查的关键字	
		http-post	12.9WE2	* http-postill台字篇	*	1MD 80	短81 0
			utt /admin/login.asp			http-post请求页表url	
			data usemame="USER"&password="PAS	55 m.		注意: ^USER^和*PASS*为字典占位符号,禁止惊召	21
			成功调度 y success			靖臣内容中包全的关键字	
	HTTPS服务类型	https-get	編曲機式	* https:get能位学典	*	280 443	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)
			uti /admin/login.exp			https-geti鼻求页面url	
		https-get-form	12合制式	* https-get-form结合字类		1月日 443	題时 0
			url /adminylogin.asp			https-get-formi黄序员宽uri	
			clata usemame=^USER^&qpassword=*PAS	\$ ⁶ .		注意: ^USER ^和 ^PASS ^为字具占位符号,禁止综合	E1
			成功明照 - success			總臣內容中包全的关键字	
		https-post-form	ilent.	* https-post-form能音字典	•	JN⊡ 443	9591 0 ⁽
			utl /admin/login.asp			https-post-form请求页面url	
			data usemame=^USER^&password=^PAS	55 ⁿ		注意: ^USER *和 *PASS *为字典占位符号、禁止综合	1
			·招助戰役 - success			政府内容中位会的关键字	
		https-head	综合情 式	* https-headiG合字曲	*	3月日 443	※时 0
			url /admin/login.asp			https-headi震灾变变url	
			data usemame=^USER^&password=^PAS	54		注意: ^USER_NII_PASS ^为学典占位符号,禁止惊动	1



系统监控				MongoDB	组合權式	¥	MongoDB组合字曲	v	3₫£B¢	0		
脆弱性管理	~				数据库名称	dmin						
⑤ 新建任务				Sybase	组合模式		sybasei日合本曲	v				
日 任务签证				Informix	组合模式	v	informix组合字典	¥				
w user				Tourset	(0.0.000)		*	1.1		2000	2761	+ 0
② 数据库检测		中间件类型		Iomcat	組合模式		lomcat组合子典	•	396	8080	201	19 0
① 安全基线检测				WebLogic	组合模式	•	WebLogic组合子典	×	第日	7001		19 0
ioi 资产管理				JBoss	組合模式	¥	JBoss组合字典	Ŧ	明日	9990	<u> (</u>) () () () () () () () () () () () () ()	12 0
⇒ ※产细管理				WebSphere	组合模式	¥	WebSphere组合字典	¥	跳口	9080	5些:	12 0
				GlassFish	組合模式	٣	GlassFish组合字典	٣	端口	4848	延日	15 O
亘 导出报表		HTTP服务类型		http-get	组合模式	*	http-get组合字典	¥	端口	80	延年	tt 0
9 模板管理	*				url /admin/lo	gin.asp			http-ge	t请求页面url		
⊙ 资产对比	*			http-get-form	组合模式	¥	http-get-form组合字典	v	端口	80	<u>Z</u> EF	H 0
う 系统管理	~				url /admin/lo	gin.asp			http-ge	t-form请求页面u	rl	
					data usernan	ne=^USER^&p	assword=^PASS^		注意: ^	USER^和^PASS	^为字典占位符	号,禁止
					成功响应 v su	uccess			响应内容	中包含的关键字		
				http-post-form	组合模式	¥	http-post-form组合字	ų v	端口	80	延日	et o
					url /admin/lo	gin.asp			http-po	st-form请求页面。	url	
					data usernam	ne=^USER^&p	assword=^PASS^		注意: ^	USER^和^PASS	^为字典占位符	号,禁止
					成功的权 ~ 51	uccess			响应内容	中包含的关键字		
				http-head	の会構式	*	http_head词合字曲	*	第日	80	3ŒF	NT 0
				intep neud	url /admin.lo	ain are	Intp included a set		http-be	ad读录页面url	~	
ascript:void(0)					un yadminyio	gin.asp			nup-ne	an Hill-J. Orthini		
											-	
			https-head	eE由標式 UIT /admin/login	Lasp	* https-bradi@S	学典 *	https-head	3 南宋茨遼url		35343 0	
				data usemamen	- USER ^ & pannword = ^ PAS	5×-		注意: ^USE	R^RD*PASS^	为字典占位符号,禁止惊骇	t i	
				版記錄匠 - succ	255			地应内容中的	自命的关键字			
			https-post	编台模式		* https-posti@B	字共 *	第日 44	3		碰时 0	
				url /admin/login	Lasp			https-postil	(市内放url			
				dàtà usemame=	- ^ USER ^ &password = ^ PAS	51		注意: ^USE	R^RD^PASSA	为字典占位符号,禁止惊る	RI	
				NAME - SHO	255			NUMBER	[142]天城子			
		国金头类型	大华	编合情式 *	大从摄像头组合字典 *	98[] 60	进时 0					
			华为	组合模式 *	华大振像头信合字曲 *	08 CIAR	BERT 0 SSL					
						the second se						

图 4.1.2.9-1 口令猜解---字典选择

字典选择配置参数说明如表 4.1.2.9-1 所示:

太 1, 1, 2, 5 I 配直多级此为	表 4.	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
中间件类型	支持多种中间件类型,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
HTTP 服务类型	支持多种 HTTP 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
HTTPS 服务类型	支持多种 HTTPS 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
摄像头类型	支持多种摄像头类型,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



4.1.2.10 口令猜解-引擎选项

⊖新建任	务				
基本配置	高级选项				
系统扫描	字典选择				
WEB扫描	引擎选项	最大线程并发数	5	对单个服务进行山令猜解的开发线程数,值越大,採测速度越快。 最大线程并发数设置[1-50]	
口令猜解					
存活探测					

图 4.1.2.10-1 口令猜---引擎选项

口令猜解一引擎选项配置参数说明如表 4.1.2.10-1 所示:

表 4.1.2.10-1 配置参数说明

参数	说明
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

4.1.2.11 存活探测--探测选项

白 新建任	务			
基本配置	高级选项			
系统扫描	探测选项			
WEB扫描		发包速率	○快速 ○ 正常 ○ 慢速 ● 自适应 ○ 自定义	(K)账: 単p300003/s 正常: 150053/s 惯账: 100053/s 自定义: 単个ip在100-5000包/s 范围
口令猜解		主机存活探测	*	
存活探测			✓ ARP	
			ICMP PING	
			TCP PING 21,22,23,25,80,443,445,139,3389,6000	
			V UDP PING 25,53,161	
		端口扫描范围	 ● 标准 ○ 快速 ○ 全部 ○ 指定 	标准: 默认摘口2000多个,快速: 1000个常用摘口,全部: 講口1-65535 指定: 単个或范围如22.1-1024,指定TCP%日: TCP:1024-65535,指定 UDP領口: UDP:1025-65535、 45点下载,了解演口详情。
		TCP端口扫描方式	CONNECT V SYN	CONNECT方式为全体搜扫描,完成TCP/IP的三次握手,速度较慢 SYN方式,只需要发达ICP SYN包即可完成检测,速度快,建议使用SYN

图 4.1.2.11-1 存活探测--探测选项

存活探测--探测选项配置参数说明如表 4.1.2.11-1 所示:

表 4.1.2.11-1 配置参数说明

参数	说明
发包速率	支持对发包速率的配置 1.快速:单 ip3000 包/s 2.正常:1500 包/s 3.慢速:1000 包/s 4.自定义:单个 ip 在 500-5000 包/s 范围

主机存活测试	对扫描主机的探测方式: ARP, ICMP PING, TCP PING, UDP PING ARP:通过 ARP 请求来实现探测,一般防火墙没法过滤 ARP 协议,成功率比 ICMP ping 高。 ICMP PING:测试网络的可达性和网络延迟。 TCP PING:使用 TCP 来向目标服务发送一个简单的 TCP 连接请求,等待服务器 的响应。通常用来测试服务器是否在线和网络延迟。 UDP PING:使用 UDP 来向目标服务发送一个简单的 UDP 数据包,等待服务器的 响应。通常用来测试网络质量和服务端的响应时间。 默认四个都勾选
端口扫描范围	1.标准:默认端口 4000 多个。 2.快速:100 个常用端口。 3.全部:端口 0-65535 4.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	1. CONNECT 方式为全连接扫描,完成 TCP/IP 的三次握手,速度较慢 2. 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

4.2 任务管理

WEBUI: 主界面 -> 脆弱性管理 -> 任务管理->任务列表

4.2.1 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

ē										
系统监控 脆弱性管理	• 任务	列表	■ 工作列表			新增+ 刷新C 至	술	8任务 ▼	搜索[回车]	
新建任务		任务 🔻	任务名称	扫描类型	扫描目标	检测结果	执行方式	优先级	任务状态	操作
□ 任务管理		230	> 172.20.54.246	系统扫描	172.20.54.246	● 高(9) ● 中(5) ● 低(5) ● 信息(4)	立即执行	+	已完成	启动
② 数据库检测		229	> 172.20.50.204xp	WEB扫描 □令猜解 系统扫描	172.20.50.204	● 高(230) ● 中(232) ● 低(51) ● 信息(35)● 弱口令(1)	立即执行	中	已完成	启动
② 安全基线检测		228	> 基线核查-172.20.50.203	安全墓线	172.20.50.203	设备数: 1 平均合规率: 31.7%	立即执行	中	已完成	启动
103 资产管理		227	> 172.20.50.203	WEB扫描 □令猜解 系统扫描	172.20.50.203	● 高(344) ● 中(517) ● 低(480) ● 信息(57)● 弱口令(0)	立即执行	中	已完成	启动
▶ 资产组管理		226	> 数据库检测-172.20.50.203	数据库检测	172.20.50.203	●高(40) ●中(197)●低(20) ●信息(2)	立即执行	中	已完成	启动
亘 导出报表		225	> win8_50.202	WEB扫描 □令猜解 系统扫描	172.20.50.202	●高(3) ●中(0) ●低(28) ●信息(12)●弱□令(0)	立即执行	中	已完成	启动
模板管理		224	> 数据库检测-172.20.50.201	数据库检测	172.20.50.201	●高(0) ●中(0) ●低(0) ●信息(0)	立即执行	中	已完成	启动
资产对比		223	> 172.20.57.42深度扫描	WEB扫描	172.20.57.42	●高(37) ●中(26) ●低(17) ●信息(5) ●弱□令(0)	立即执行	中	已完成	启动
系统管理		218	> 172.20.57.42标;崔扫描	WEB扫描 □令猜解 系统扫描	172.20.57.42	●高(0) ●中(2) ●低(29) ●信息(3) ●弱口令(0)	立即执行	÷	已完成	启动
		217	> 172.20.57.42dcbox	WEB扫描 □令猜解 系统扫描	172.20.57.42	●高(92) ●中(65) ●低(34) ●信息(9) ●弱口令(0)	立即执行	中	已完成	启动
		216	> 172.20.57.51	WEB扫描 □令猜解 系统扫描	172.20.57.51	●高(128)●中(68) ●低(62) ●信息(16)●弱口令(0)	立即执行	÷	已完成	启动
		215	> 172.20.52.230AS	WEB扫描 □令猜解 系统扫描	172.20.52.230	●高(124)●中(59) ●低(183)●信息(35)●弱口令(0)	立即执行	低	已完成	启动
		214	> 172.20.52.230	系统扫描	172.20.52.230	● 高(4) ● 中(10) ● 低(27) ● 信息(13)	立即执行	÷	已完成	启动
		213	> 172.20.54.172	系統扫描	172.20.54.172	●高(32) ●中(63) ●低(26) ●信息(25)	立即执行	÷	已完成	启动
		212	> 172.20.54.202	系統扫描	172.20.54.202	●高(11) ●中(11) ●低(24) ●信息(10)	立即执行	÷	已完成	启动
		211	> 172.20.57.42	系统扫描	172.20.57.42	● 高(128) ● 中(65) ● 低(26) ● 信息(15)	立即执行	÷	已完成	启动

图 4.2.1-1 任务列表总览



表 4.2.1-1 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,存活探测,安全基线
扫描目标	显示任务中所有的扫描目标
优先级	显示当前任务的优先级,有高中低三种
任务状态	包含排队等待,正在检测,已完成,已停止,已暂停,正在处理
检测结果	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存活主机数,基线任务可以查看设备数和平均合规率, 口令猜解可以查看扫描的口令数
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

4.2.1.1 任务列表操作

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:

210	> 数据库检	测-172.20.52.89 数据库	金测	172.20.52.89	● 高(0) ● 中(0) ● 低(0) ● 信息(0)	立即执行	中 已完成	启动
209	~ 已有靶机	N扫描 WEB扫	描 □令猜解 系统扫描	172.20.50.201	,172.20.50.200,172 ● 高(2071)● 中(1909)● 低(642) ● 信息(163)●	弱口令(0) 立即执行	商 执行中	暂停 停止
子任务ID	任务类别	开始时间	结束时间	检测耗时	结果信息	检测进度	語	R/fe
440	WEB扫描	2023-05-06 18:48:06			检测网页数:9733 高危:301 中危:225 低危:400 信息:1		执行中 94%	详情
439	口令猜解	2023-05-06 18:48:06	2023-05-06 19:07:33	19分27秒	弱口令数量:0		已完成 100%	详情
438	系统扫描	2023-05-06 18:35:47	2023-05-06 18:52:45	16分58秒	主机数:3 高危:1770 中危:1684 低危:242 信息:36		已完成 100%	详情

图 4.2.1.1-1 扫描任务执行状态

4.2.1.2 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 4.2.1.2-1 所示:



系统监控	结果详情				返回任务委
> 脆弱性管理 ^	主机列表 漏洞列表	請口列表 历史执行记录			
新建任务	风险级别 🔺 濃	调合称	漏洞所闻分类	总计	172 20 50 204
□ 任务管理	高风险	licrosoft Windows RDP 远程代码执行漏洞(CVE-2012-0002)(MS12-020)【	其它	1	
② 数据库检测	高风段 5	MB中的漏洞可能允许远程执行代码(ms09-001) [原理扫描]	其它	ì	
② 安全基线检测	高风险	ficrosoft Windows SMB服务器多个漏洞(ms17-010) 【原理扫描】	默认探测	ì	
acx 资产管理	高风脸	licrosoft Windows SMB / NETBIOS NULL会话身份验证绳过漏洞	其它	1	-
壹 资产细管理	高风脸	HP PostgreSQL扩展拒绝服务漏洞 (CVE-2015-4644)	其它	1	0 100 200 300 400 500
三 导出报表	高风脸	HP 安全漏洞 (CVE-2017-9226)	缓冲区溢出	1	漏洞总数 (个)
模板管理 、	高风险	HP 多个版本安全漏洞(CVE-2004-1064)	其它	1	漏洞风险分布
资产对比 🔹	高风险	测到目标操作系统已停止维护【原理扫描】	默认探测	1	
系统管理 >	高风险 A	pache HTTP Server 癒中区错误周洞(CVE-2021-39275)	缓冲区溢出	1	高风险[227]
	高风脸	hpMyAdmin 多个末明濡洞(CVE-2007-0203)	输入验证	1	(低风险[20]
	高风险	HP 5.2.6 'fastcgl.c' 缓存区溢出漏洞(CVE-2008-2050)	缓冲区溢出	1	
	高风脸	HP crypt函数缆冲区错误漏洞(CVE-2011-3268)	缓冲区溢出	1	
	高风险P	HP WDDX扩展缓中区错误漏洞(CVE-2016-3141)	缓冲区溢出	1	
	高风脸	HP 'bcpowmod' 函数安全潇洞 (CVE-2016-4538)	输入验证	1	*

图 4.2.1.2-1 系统扫描漏洞详情

点击漏洞会显示改漏洞的相应信息,编号、风险级别、年份、描述、解决方法、检测详 细等,如图 4.2.1.2-2 所示:

💌 数据安全检查	工具箱系统						0 0 20140022 103815 A 868188 + 0 85
日 机邻性检测剂	(① 制限性批判 / 生任务管理						
= (1992)	主机利用 建用利用	第四判案 历史执行记录				I INSEMDLY	
A 政策年位回	MARINE	* #R88	Apache httpd	输入验证错误。	(旅河 (CVE-2017-15715) (1論入验证)		×
··· 安全县场险制			94 1 5	1101366			
			风险级别	来政治			
日 新設行家介绍	ESSE .	Apoche httpd 加入验证时间期间(0	469	2017			
	ESSE .	F5 Algina 编句的 建油油 建制 (CVE-20)	CVE	CVE-2017-157	5715 Yan watan su dikiwa ili waki tan su da su da su		
	E223	Apache HTTP Server BPS Antes	CNCVE	CNCVE-20171	115715		200 250 200 150 400 450 500 550 000
	ESSER.	Ciracle MySQL/MariaDE ServertER	CNNVD	CNNVD-2017	710-1011		anex (1)
	E3333	MarlaD目 = 全部町 (CVE-2022-274	Bugtraq ID	103525			
	EXC.	ManaDe SQUEARER (CVE-2022	161.K	Apache httpd: Apache httpd	d是美国同物語(Apache)软件基金会的一款专为现代操作系统开发和维护的开提HTTP服务器。 d 24.0版本型24.29版本中存在安全漏洞。取出者可通过向目标系统发送特制的文件利用说漏网络过安全限制。		
	10000	Microsoft SQL IDEMS BUILING	解决办法	目前厂商已发布 https://httpd.	布升級补丁以体棄業用。 料丁研取链接: 1.apache.org/security/vulnerabilites_24.html		IIII 205420(3322)
		Semble Collector House and Balling	10.962.05				100 (+ 162/01/464/8) 100 (- 162/01/164/8) 100 (- 162/01/164/8)
	E3275	MariaDil 医脊髓脊髓炎 Ratifi (CVS-2		检测速度	apache:http_server 2.4.6 >= 2.4.0		C (22(1199)
	E3223	Operaal OpenSSL 地图问题编码 (C	v		apachehttp_server 2.4.6 <= 2.4.29		
	1552A	VMware ESXL, Workstation@Funit	an an	194Cl	80		
	E3323	Swagger API # SPECIFICATION 1893	-	服务	http		
	E3273	Memcached growth (CVE-2017-		10-52	TCP		
	EXC.	Explat the HER STREAM SCVE-2018-1		重机地址	172.20.54.28		
	1000	Apache Tomcet IT RETEREN (CVI		廣闲状态	H4 ·		
	E500	Vinware ESR, Workstation/CFusio	20				
	-	MariaDE @ 2.800 (CVE-2022-320	0.	检测语题	apachernttp_server 2.4.6 >= 2.4.0 apacherhttp_server 2.4.6 <= 2.4.29		
	-	Gracie MySGL/MariaDB Server CB		Dec.	80		
	1000	Microsoft SQL RDBMS BITERSPELE	the second s	服務	http://www.com/article/art		-

图 4.2.1.2-2 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 4.2.1.2-3 所示:



<u>10</u>						
會 系统监控	结果详情					返回任务列表
◎ 鵜弱性管理 ^	网站列表 漏洞列表 漏洞目录树 历史执行记录				WEB扫描详情	
新建任务	<u>ь</u> ~	风险级91	濃潤名称	息计	-	
日 任务管理	h http://172.20.50.204/ 3 3 26	高风段	跨站脚本攻击漏洞 (编码)	1	网站域名	http://172.20.50.204/
② 数据库检测		高风脸	(結接注入	1	IPTER	172.20.50.204
O DARKIAN					网站服务器	Apache/1.3.24 (Win32) PHP/4.1.3-dev
O XIIISTAN		高风段	框架钓鱼	1	网站标题	AppServOpenProject
10 资产管理		中风脸	启用了目录列表	42	网站编码	ISO-8859-1
壹 资产细管理		中风脸	域名访问限制不严格	1	网站语言	PHP/4.1.2
三 导出报表		(EEGUA	文件路径泄漏	20	网站物理	局域网-对方和您在同一内部网[172:16.0.0-172:31.255.255]
◎ 模板管理 🗸		低风险	发现电子邮箱	4	网页总数	319
⊙ 资产对比 ∨		(EDQUA)	X-Frame-Options头未设置	1	漏洞风险分布	
⊙ 系统管理 ∨		(EEXIR)	HTTP Referrer-Policy头缺失	1		
		低风险	HTTP X-Download-Options头缺失	1		
		(EEFALIE)	HTTP X-Content-Type-Options头缺失	1		高风脸[3]
		(EE)QAD	启用了危险的Method	1		((风)((1)) 【信息[26]
		(EDGRO)	HTTP X-Permitted-Cross-Domain-Polici	1		
		低风险	启用了危险的Method (TRACE)	1	*	

图 4.2.1.2-3 Web 扫描漏洞详情

点击漏洞列表中的漏洞,显示该漏洞的相关信息,并可以对其进行验证操作,如图 4.2.1.2-4 所示:

8134383 •• 2039(2)/ • 2 4623 55243(6)/ • 46434 •• 4043(2) • 246438 •• 4043(2) • 236458 •• 2039(2) • 10139/* •• 20	2 소등 전 ARTER M Management ARTER Management ARTER Management ARTER (Concellation) ARTER (Concellation)	Cybrotech C Registr es starta painta	y/SrokttpServer 1.1 このなび そのないまた、Cylin とないまた、Cylin 1.5世紀であった。 1.5世紀であった。 単語になった。 単語になった。 単語になった。 1.5世紀であった。 単語になった。 単語になった。 1.5世紀であった。 単語になった。 1.5世紀であった。 1.5世紀でののののの。 1.	0.3把込却不均主用用(A3 對法却本 (XS5) rishtblervel集/面の456450(日期)-更用于非新 时间或用用之人生用的/vel#FamilyA、一局容中(A), 面積 2004年10人生用一致人一局容中(A), 面前 2004年10人生用一致人一的分子(A), 用用 服用、完全的Coll State Schollero, IRECSSDIK 医的工具的工具的工具的工具的工具的工具的工具的工具的工具的工具的工具的工具的工具的) (成取/写AC/SPOR2量的透像限制構築 (2018)(原用時中: 新人房内房已的包裹 5、它面的基本等なも含いいもの方向至初の発展 音、調査室可にいるの方向至初の発展 Flash自用の適用を通行な法,从用 Charlogites,Et HTTP/1.1 	 Cybrotech CyBroHetps/ mrSA気を考知7, 第中国人一彩を書ける。当年 回惑中的内容。 年に上の方形内 名の 中国人の名の方の名の (本)上の方形内 名の (本)上の方形内 名の (本)上の方形内 (本)上の方形内 (本)したの	ever 1.0.387+99094687+889, 59 ever 1.0.387+99094687+889, 59 ever 1.0.387+99094494 ever 1.0.387+99094 ever 1.0.397+9904 ever 1.0.387+9904 ever 1.0.397+9904 ever 1.0.397+9904 ever 1.0.397+9904 ever 1.0.397+9904 ever 1.0.397+9004 ever 1.	× 增加為東可保助 及使代码就会说 100	1.59 200 230	200 333 0 BRIER (5
Active Active Active Resident Active Active Active	APATELINE MEMORYCE ADDELINE MEMORYCE Coperation Cyfeinerigiawrer 1.02 Coperation Cyfeiner 1.02 Coperation	Cybrotech C Albesta apr statute 1380/754 1380/756	yBroHttpServer 1.1 Cybrotech Cybr 世帯型は東京同志 オートレート オート	0.3時込期本改主用用何(A3) 開始期本 (XSS) の10105mmの場合型(2)のからの日の一の一方金成年 利用温度的ないための日の一の一の一方金成年 利用温度のための日の一の一の一方金成年 用用、用なるの日本の一の一の一の一の一の一の 用用、用なるの日本の一の一の一の一の一の一の一の 用用、用なるの日本の一の一の一の一の一の一の一の 用用、用なるの日本の一の一の一の一の一の一の一の 用用、用なるの日本の一の一の一の一の一の一の一の一の 用用、用なるの日本の一の一の一の一の一の一の一の一の一の 用用、用なるの日本の一の一の一の一の一の一の一の一の 用用、用なるの日本の一の一の一の一の一の一の一の一の 用用、用なるの日本の一の一の一の一の一の一の一の 用用、用なるの日本の一の一の一の一の一の一の一の一の 用用、用なるの日本の一の一の一の一の一の一の一の一の一の 用用、用なるの日本の一の一の一の一の一の一の一の一の一の 用用、用なるの日本の一の一の一の一の一の一の一の一の一の一の 用用、用なるの日本の一の一の一の一の一の一の一の一の 用用、用なるの日本の一の一の一の一の一の一の一の一の一の一の 用用、用なるの日本の一の一の一の一の一の一の一の一の一の一の 用用、用なるの日本の一の一の一の一の一の一の一の一の一の 用用、用なるの日本の一の一の一の一の一の一の一の 用用、用なるの日本の一の一の一の一の一の一の一の 用用、用なるの日本の一の一の一の一の一の一の一の一の 用用、用なるの日本の一の一の一の一の一の一の一の一の一の 用用、用なるの日本の一の一の一の一の一の一の一の一の一の 用用、用なるの日本の一の一の一の一の一の一の一の一の一の一の 用用、用なるの日本の一の一の一の一の一の一の一の一の一の 用用、用なるの日本の一の一の一の一の一の一の一の一の一の一の 用用、用なるの日本の一の一の一の一の一の一の一の一の一の一の一の 用用、用なるの日本の一の一の一の一の一の一の一の一の一の一の一の一の 用用、用いて、用いて、用いて、用いて、用いて、用いて、用いて、用いて、用いて、用) (市内/用入く分のの運動)通信(取得)通信 (市内)用用一 (市内)用用一 (市内)用用用 (市内)用用用用 (市内)用用用用 (市内)用用用用 (市内)用用用 (市内)用用 (市内)用 (市	 Cybrotech CyBroHttpS- eres時後後の万 面中違入一紀念着代約、当年 回用一向59時、 年に急が花気味相が用中構築 	• สมของสม even1038749939687488, 55 5-25585587, ค.).5000554993 สค.	× 相対政策で何約 2世代的政治会社	150 200 230	200 JSN 4 BRIDEN (1
R.6.13 P.0.615 P.0.615 P.0.615 R.6.618 R.0.616 R.0.616 P.0.616 R.13.7 R.0.317 R.0.317 R.0.317 R.13.7 R.0.318 R.0.317 R.0.317 R.0.317 R.13.7 R.0.318 R.0.318 R.0.317 R.0.317 R.13.7 R.0.318 R.0.318 R.0.318 R.0.317 R.13.7 R.0.318 R.0.318 R.0.318 R.0.318 R.13.7 R.0.318	RATES REALIST REALIST REALIST A REALIST Control A REALIST Control A REALIST Control B REALIST Control	Cybrotech C Riddini Rife Rife Sile Sile	SyBroHitpServer 1.1 Contact CyBin Servership Se	0.33時法部本攻主無用何(A3 首先部本 (XSS) (14)(4)(4)(4)(4)(4)(4)(4)(4)(4)(4)(4)(4)(4) (東京/四人に分かって重約)清保研究務 (国内は同時)、 個人3回月から2回 (国内にの日本)、 日本の日本の日本の日本の日本 (日本の日本の日本の日本の日本の日本の日本) (日本の日本の日本の日本の日本の日本の日本) (日本の日本の日本の日本の日本の日本) (日本の日本の日本の日本の日本) (日本の日本の日本の日本) (日本の日本の日本)(日本の日本)(日本の日本)(日本の日本)(日本)(日本)(日本)(日本)(日本)(日本)(日本)(日本)(日本)(4、Cybrotech CyBrolittyss 即代码是未成为了。 如何是几人————————————————————————————————————	 сененая errer 1.0.1gt=арадный=й, б/ селеная селеная	× 但沈政者可保助 及世代到政会地	156 200 228	300 135 BRIER (1
HEAR AND A CONTRACT A	Autopie Cphronicol Cyliniarity/downer 10.2 Cphronicol Cyliniarity/downer 10.2 United Intercology CARREDOLLXAMI Highlight Antonemotical	Cybrotech C Riddste star starty Ja Istarto	yBroHttpServer 1.1 Cybrotech CyBre Breasestapith 1. 時後日本の政策 2. 市場の中のないの 1. 日本の中のないの 2. 市場の中のののの 1. 日本の中のないの 2. 市場の中のののの 1. 日本の中のないの 2. 市場の中のないの 1. 日本の中のないの 2. 市場の中のないの 1. 日本の中のないの 1. 日本の本の 1. 日本の本の 1. 日本の本の本の 1. 日本の本の本の本の 1. 日本の本の本の本の本の本の本の 1. 日本の本の本の本の本の本の本の本の本の本の本の本の本の本の本の本の本の本の本の	0.33年4年期年代本設立無限(人名) 1988年(XSS) 10511054194月24日、2018年10月4日、2018年10月4日 1月1日2日日日、2018年10月4日日、2018年11月4日 1月1日2日日日、2018年11月4日日、2018年11月4日 日本設造やあたりまた、2018年11月4日、2018年11月4日 日本設造やあたりまた。2018年11月4日、2018年11月4日 日本設造やあたりまた。2018年11月4日、2018年11月4日 日本設造やあたりまた。2018年11月4日、2018年11月4日 日本設造やあたりまた。2018年11月4日、2018年11月4日 日本設造やあたりまた。2018年11月4日、2018年11月4日 日本設造やあたりまた。2018年11月4日、2018年11月4日 日本設造やあたりまた。2018年11月4日、2018年11月4日 日本設造やあたりまた。2018年11月4日、2018年11月4日 日本設造やあたりまた。2018年11月4日、2018年11月4日 日本設造やあたりまた。2018年11月4日、2018年11月4日 日本設造やあたりまた。2018年11月4日、2018年11月4日 日本設造やあたりまた。2018年11月4日、2018年11月4日 日本設造やあたりまた。2018年11月4日、2018年11月4日 日本設造やあたりまた。2018年11月4日、2018年11月4日 日本設造やあたりまた。2018年11月4日 日本会造やあたりまた。2018年11月4日 日本会造やあたりまた。2018年11月4日 日本会造やあたりまた。2018年11月4日 日本会造やあたりまた。2018年11月4日 日本会造やあたりまた。2018年11月4日 日本会造やまたりまた。2018年11月4日 日本会造やまたりまた。2018年11月4日 日本会造やまたりまた。2018年11月4日 日本会造やまたりまたりまた。2018年11月4日 日本会造やまたりまた。2018年11月41日 日本会造やまたりまた。2018年11月41日 日本会造やまたりまたりまままままままままままままままままままままままままままままままま) (原語/場入くらいの変更が通信能研発 の)地域内面対、最入到向西の的思想 5、世紀が最高度なた者をがやら改造 2、調査室可しょきの内面型的高級を通行な法、人の Flaving 門的高級を通行な法、人の Charloget%32 HTTP/L1	4、Cybrotech CyBroHttpSA mc石泉鉄水地水行。 面中磁入一税を置け扱。血草 市場入一税を置け扱。血草 中国の内容。 中国の同時、 中国の同時、	error 1.0.2度平中均均500年8月、約 8中205年5月11、約入前1005月9日2 月15。	学校成准者可维助 法责代码就会被	150 200 230	300 ISB 1000281 (
	Cyberiech Cybroshtydower (18.3) IRIZIER (Coner) IRIE Cology Chiefers (18.3) IRIE Colog	泉絵豊田	日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日	rdHttp/arver着美国公社のなない公司的一部用子中級制 利用法規則に入止性的がいを結果面が「ALL」 発展に満定する。有利には、人一部品を引いた。 基礎に加入した性がでは、一部品を引いた。 気がしたが、またした、それがあ、人間に入し、運用 うたいためでは、それがあ、人間に入し、運用 うたいためでは、それがあ、人間に入し、運用 トロングーングロングーングロングーングロングーン トロングーングロングーングロングーングロングーン トロングーングーングーングーングーングーン トロングーングーングーングーングーン トロングーングーングーングーン トロングーングーングーン トロングーングーングーン トロングーングーン トロングーングーン トロングーングーン トロングーングーン トロング トロン	換数/用入心(加口支盤的遺情服務構成 20世紀時期時、 細人為約2000回線 5、它論的基本要な出意者のWeb交流 意、要素至可には彼の現代思想的時候的 月ahh自用的環境用時近行改造、从用 Chongeth3E HTTP/1.1	4、Cybrotech CyBroHttp5 當行局勢力被执行。 當中違入一股意變代码。当年 当時一的内容。 等該到原取時 他的用户 痛養	erver1.0.3版本中存在預始基本現象,54 和P2页集成页面时,最大批Web页面中的最	程改造者可做助 2番代码就会被	150 200 230	309 350 1980:::RI
15. ²⁴ 15. ²⁴ 15. ²⁴ 15. ²⁵ 15. ²⁵	田正道子 (Orien) 田正道子 (Orien) 田田(Orien)ののからのののののののののののののののののののののののののののののののののの	■19 新决方法 [38]开始	Cyloraten Uym 高速は単規同算体 1.現地様率改造構 以不、从市区542 高速 2.思想用の可以使 建築用の可以使 建築用の可以使 建築用の可以及 建築用の可以及 2.思想用の可以 建築用の可以 建築用の可以 建築用の可以 2.思想用の可以 2.思述目的での可以 2.思想用の可以 2.思想用の可以 2.思想用の可以 2.思述目のでの可以 2.思述目のでの可以 2.思述目のでの可以 2.思述目のでの可以 2.思述目のでの可以 2.思述目のでの可以 2.思述目のでの可以 2.思述目のでの可以 2.思述目のでの可以 2.思述目のでの可以 2.思述目のでの可以 2.思述目のでの可以 2.思述目のでの可以 2.思述目のでの可以 2.思述目のでの可以 2.思想用の 2.思想用の 2	の中ロションサイン 「中国ションサービー」 「日本のション」 「日本の 「ー 「日本の 「ー 「日本の 「日本の 「 「日本の 「 「 「 「 「 「 「 「 「 「	目前は、ArLineで変更が強いためで、 ないためで、 ないためで、 ないためで、 ないためで、 ないためで、 ないためで、 ないためで、 ので、 ないためで、 ので、 ので、 ので、 ので、 ので、 ので、 ので、 の	、 Cyslotern Cyslonttips 副代码此会後決行。 国中國人一股改要代码。当年 回用户的内容。 毎日达到印刷知何的一個書	erer LLAR FORMER AND, SS	他(又由著 6) ((正)) 5.巻(-(250)():))(() 100	150 200 230	300 ISI BREA
	Emile Codey, CARPESCIELA XIII Hegish (colour-colo) Hegis	新(水方)点 1318(〒0)	1.週回時本3.00回 2.周延期本3.00回 取行、从間近時 意志 1.週間用中間以復 2.週間用中間以復 違い江途用中輸入 調成用用	は加速度の高額には、日本(1)、10-40/-0000(1)・50-40/-0000(1)・50-40/-0000(1)・50-40/-0000(1)・50-40/-0000(1)・50-50(1)-50-50(1	Motionallingで、新人員内田中心思想 S、它論語重要意定出着向Webの支援 使、算著至可以傳动殘反呈现結構相 Flash位何的道商傳過行攻击。从而 Chacipthiste HTTP/1.1	部(1946)大学校大学。 第一連入一股容量代码,当年 目前一股内容, 目前上股环联系化的用户信息	BPOJSARSH, WAEWebRSHeb3	5.@rf:5500.eHt	150 200 250	309 158 BRER
	Hittp://dots/united/2015 Hittp://dots/united/2015 Hittp://dots/united/2015 United/2015 United/2015 Realized/2015 Market/ Market/2015 Ma	新决方法 E3881年48	2017、5000210 方言: 1.延登用户可以使 2.思想用户可以使 建议过度用户站人 遵保URL 商ば用例	## ALL ##1197822. ## ALL ##119782 ##119782 ## ALL ##11978 ## ALL ##11978 ## ALL ###11978 ## ALL ###11978 ## ALL ############################	奈,要基至可以確認局法呈現地無地 Flash位用的構用単進行改造、从用 C/script%3E HTTP/1.1	5月中的内容。 19年达到这家城他的用户信息	En.	100	150 200 250	309 350 16902-18
	NAME RECORDER (n) HERDER HONORANNE (D) MERINE HONORANNE (D) MERINE X MERINE (D) MERINE X MERINE (D) MERINE (D)	新花水方3点 13881年18	2.思想用中可以使 確以过速用中域人 應用URL 向は用用	世界JavaScipt, VBScipt, ActiveX, HTML開催者3 Aff308年, 502月中196年年後のA部第以5週末年金10, http://1722.05.54.1318428/ GPT //522.05.54.1318428/ GPT //522.05.54.1318428/ Hott: 1722.05.51.1318428/ Hott: 1722.05.51.1318428/	Plash@考虑的意义的,从而 C/script%3E HTTP/1.1	第15到37和M他的很产品。	en.	106	150 200 230	300 250 Rifterr
	HTTLE-H-lostnamedicas an Relationer Material Contractions and Contractions and Contractions and Contractions	新 <i>庆方法</i> 日期詳報	建位1216月中始入 環境URL 別は市例	A 的ない第一切已用一切5年年46.入都第4.5次第千日全的。 http://1722.05.41.31342426 GET /%3Ckoriptf%3Eakert"ghbethr_sssteest7(%) Accept.** Referen: http://172.05.41.313428/ Host: 772.05.4135428	C/script%3E HTTP/1.1					RREA
	HARDAN MARANARA (M REFEX MENDINETAN REFERENCES	E1985E1	應用URL 附述用例	http://172.20.54.1318428/ GET /%3Cscript%3Ealert("gfsbrthr_xsstest")%3 Accept */* Referen: http://172.20.54.1318428/ Host: 172.20.54.1318428	C/script%3E HTTP/1.1					
	Production and (p) matrix and institute from any distribute from		漏洞URL 购试用例	http://172.20.54.131:8428/ GET /%3Cscript%3Ealerti*gfsbrthr_xsstest1%5 Accept: /* Referer: http://172.20.54.131:8428/ Host: 172.20.54.131:8428	C/script%3E HTTP/1.1					
	anner 2. Millio (1970) Millio 7.795 Millio (1970) Anner 1970		詞试用例	GET /%3C script%3Ealert("gfsbrthr_xsstest")%3 Accept: */* Refere::http://172.20.54.131:8428/ Host:172.20.54.131:8428	C/script%3E HTTP/1.1					
	MGMSBMFFF			Referer: http://172.20.54.131:8428/ Host: 172.20.54.131:8428						
	In statistic states							1		中見地(
				Connection: Keep-Alive User-Agent: Mozilia/5.0 compatible; MSIE 9.0	Windows NT 6.1; WOW64; Tride	ent/S.0				M (AR(33)
				Accept-Encoding: gzip,denate						
ENTITE OF	#卡伯田田和丁 川 田		94338	會配值世紀 <script></script>						

图 4.2.1.2-4 漏洞详细

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 5.2.1.2-5 所示:

结果详情					返回任务列
主机列表 弱口令列表	历史执行记录				
主机名称		服务	端口	用户名	密码 ●
172.20.50.204		smb	445	Administrator	123
总计1条记录					每页显示 25 ▼ 〈 1 〉

图 4.2.1.2-5 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 4.2.1.2-6 所示

吉果详情				通知	任务列表
存活列表	历史执行记录				
每页显示	25 *			一鍵任务下发 一键转为	资产
存活IP		▼ 存活端口	协议	服务/服务旗标	
172.20.5	4.99	80	TCP	http	
		443	TCP	https	
		3306	TCP	mysql	
		4298	TCP	http	
		8080	TCP	http	
		40000	TCP	ssh/openbsd:openssh:7.4 OpenSSH	
172.20.5	4.98	80	TCP	http	
		443	TCP	https	
		3306	TCP	mysql/mariadb:mariadb:10.2.17 mariadb	
		4298	TCP	http	
		8080	TCP	http	
		40000	TCP	ssh/openbsd:openssh:7.4 OpenSSH	
172.20.5	4.97	22	TCP	ssh	
		80	TCP	http	
		443	TCP	https	
		3306	TCP	mysql/mariadb:mariadb:10.2.17 mariadb	
		8002	TCP	http	
		8009	TCP	http	
		8080	TCP	http	
		8100	TCP	http	

图 4.2.1.2-6 存活列表

仅基线可显示: 主机列表、核查项, 以及历史执行记录, 如图 4.2.1.2-7 所示



图 4.2.1.2-7 安全基线

4.2.1.3 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

4.2.1.4 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,任务名称和扫描目标不支持编辑,如下

Ξ			
 ● 系统监控 ○ 総弱性管理 ^ 	Q 任务列表 ■ 工作列表 高线服務 ct 在线服務 C 编辑 / 翻除 x 复制 Q 新常 +	刷新ご	全部任务 * 搜索[回车]
計 新建任务	□ 任务… ▼ 任务名称 ◆ 扫描光型 扫描目标 检测结果	执行方式	优先级 任务状态 操作
□ 任务管理	✓ 230 > 172.20.54.246 系統扫描 172.20.54.246 ●商(9) ●	▶(5) ●低(5) ●信息(4) 立即执行	r 中 已完成 _{启动}
② 数据库检测	□ 合称: 基线线查-172.20.50.203 所属用户: admin □令猜解 系统归描 172.20.50.204 ● 商(230) ● *	▶(232) ● 低(51) ● 信息(35)● 弱口令(1) 立即执行	i 中 已完成 _{启动}
② 安全基线检测	□ 228 → 基线绘査-172.20.50.203 安全基线 172.20.50.203 设备数: 1 平均	9合规率: 31.7% 立即执行	i 中 已完成 _{启动}
四 资产管理	227 > 172.20.50.203 WEB扫描 □令猫解 系统扫描 172.20.50.203 ●商(344) ● 5	Þ(517) ● 低(480) ● 信息(57)● 弱口令(0) 立即执行	r 中 已完成 _{启动}
壹 资产组管理	□ 226 > 数据库检测-172.20.50.203 数据库检测 172.20.50.203 ●高(40) ● 第	▶(197) ● 低(20) ● 信息(2) 立即执行	r 中 已完成 启动
亘 导出报表	□ 225 > win8_50.202 WEB扫描 □令猜解 系统扫描 172.20.50.202 ●高(3) ●	▶(0) ●低(28) ●信息(12)●弱口令(0) 立即执行	i 中 已完成 启动
	□ 224 > 数据库检测-172.20.50.201 数据库检测 172.20.50.201 ● 商(0) ● 5	▶(0) ●低(0) ●信息(0) 立即执行	i 中 已完成 启动
资产对比 *	□ 223 > 172.20.57.42深度扫描 WEB扫描 □令猜解 系统扫描 172.20.57.42 ●商(37) ●	中(26) ●低(17) ●信息(5) ●弱口令(0) 立即执行	i 中 已完成 _{启动}
⊙ 系统管理 ✓	□ 218 > 172.20.57.42标准扫描 WEB扫描 □令猫解 系統扫描 172.20.57.42 ●高(0) ● =	Þ(2) ●低(29) ●信息(3) ●弱口令(0) 立即执行	r 中 已完成 _{启动}
	□ 217 > 172.20.57.42dcbox WEB扫描 □令猫解 系統扫描 172.20.57.42 ●高(92) ● 5	▶(65) ●低(34) ●信息(9) ●弱口令(0) 立即执行	中 已完成 启动
	□ 216 > 172.20.57.51 WEB扫描 □令猜解 系统扫描 172.20.57.51 ●高(128) ● 3	Þ(68) ●低(62) ●信息(16)●弱口令(0) 立即执行	r 中 已完成 启动
	□ 215 > 172.20.52.230AS WEB扫描 □令猜解 系统扫描 172.20.52.230 ●高(124) ● 3	Þ(59) ●低(183)●信息(35)●弱口令(0) 立即执行	ř 低 已完成 _{启动}
	□ 214 > 172.20.52.230 系統扫描 172.20.52.230 ●商(4) ● 4	Þ(10) ●低(27) ●信息(13) 立即执行	i 中 已完成 启动
	□ 213 > 172.20.54.172 系统扫描 172.20.54.172 ●商(32) ● 4	Þ(63) ●低(26) ●信息(25) 立即执行	i 中 已完成 启动
	212 > 172.20.54.202 系統扫描 172.20.54.202 ●商(11) ●	▶(11) ●低(24) ●信息(10) 立即执行	r 中 已完成 启动
	□ 211 > 172.20.57.42 系統扫描 172.20.57.42 ●商(128) ● =	Þ(65) ●低(26) ●信息(15) 立即执行	r 中 已完成 启动



-				
會 系统监控				
 · · · · · · · · · · · · · · · · · ·	□ 新建任务			
D. Mithing	基本配置 高级选项			
山 新建社务	新建任务类型	✓ 系統扫描 Web扫描 □ 今補	解 仅存活探测	* 提示:如勾选仅存活探测,则不进行漏洞扫描,仅探测资产存活状态和端口开放情况
目 任务管理	扫描目标方式		= 1	
② 数据库检测			7/	▲ k-1++ = +=.a==+0.75
⑦ 安全基线检测	日通日标			▲ 二面目 町場 号がしこ: IPv4示例:192.168.1.100,IPv6示例: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
				IP版示例: 192.168.1.0/24,192.168.2.1-254,192.168.3.1-192.168.3.254,192.168.1.* 據名示例: www.example.com
10 资产管理				URL示例: http://192.168.1.100/.https://www.example.com/ http://[юсосооссооссооссооссооссооссооссооссоос
壹 资产组管理				排除IP或IP段: !192.168.1.1/24,!192.168.1.1-255,!192.168.1.1 类似192.168.3.cc、192.168.bb.cc、192.aa.bb.cc格式将会被视为域名,清确认后提交
亘 导出报表				多个之间以英文逗号()或换行分隔
○ 模板管理 ~	任务名称			*提示:请靖写任务名称,长度在[1-40]字符之间
○ 第 产 初世 ×	执行方式	立即执行 ▼ *提示	1: 请选择执行方式	
	系统漏洞模板	全部漏洞扫描 * *提示	: 请选择漏洞插件模板	
◎ 熱號管理 *	检测模式	标准扫描 * 标准	封油:默认选择标准端口的端口范围,采用主机存活制	则断、端口扫描、服务判断、漏洞测试的步骤对扫描目标进行完整的安全扫描
		決通	193曲: 伏迷的对归悔日标进行主机存活、 續口處守抹淡 193描: 默认选择全部猜口的端口范围,采用主机存活判 對3描:利用配置好的用户名密码列表对主机进行登录后	9 呵听,頭口扫描,服勞判断、漏洞测试的步骤对扫描目标进行完整的安全扫描 約9安全扫描
	调试模式	マーを行った。	f启,则记录目标详细播件执行日志。	
	执行优先级别	中 *提示	: 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
	分布式引擎	默认 * * 默认 * * 默认 * 注意	1: 系统将根据引擎的负载情况,智能选择工作引擎 loo 第: 下发口令猜解任务若使用非默认字典,系统将自动进	cal:系统将会选择本 <mark>地引擎</mark> 选择本地默认引擎
	告警模板	无 * 捲玩	:: 告警发送配置,猜到(系统管理>任务告警)下设置	
		提交		

图 4.2.1.4-1 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

4.2.1.5 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

-													
系统监控 能弱性管理 ^		♀ 任务列表	E 工作列表 高线报	表 0; 在线报表记 \$	ali · · · · · · · · · · · · · · · · · · ·	复制化	新增÷	刷新さ	至	全	部任务 *	搜索[回车]	
新建任务		任务	▼ 任务名称	1 扫描类型	扫描目标		检测结果			执行方式	优先级	任务状态	操作
□ 任务管理		230	~ 172.20.54.246	系统扫描	172.20.54.246		●商(9) ●中(5) ● (氏(5) ● 信息(4)		立即执行	¢	已完成	启动
② 数据库检测		子任务ID	任务类别开始时间	结束时间	检测耗时	结果信息			检测进度			ŧ	RYF
② 安全基线检测		479	系统扫描 2023-05-08	14:48:42 2023-05-08 14:55:	01 6分19秒 ∃	主机数:1 高危:9	中危:5 低危:5	信息:4	No.		E	100%	详悟
四 资产管理		229	> 172.20.50.204xp	WEB扫描 口令猜解 系统扫	描 172.20.50.204		● 商(230) ● 中(232) ● 低(51) ● 信息(35) - 弱口 (1)	立即执行	中	已完成	启动
壹 资产细管理		228	> 基线核查-172.20.50.203	· 安全基线 确定册	除所选项?				×	立即执行	中	已完成	启动
三 导出报表		227	> 172.20.50.203	WEB扫描□令猜解				取消 載	tik (0)	立即执行	÷	已完成	启动
模板管理 *	1	226	> 数据库检测-172.20.50.2	03 数据库检测	172.20.50.203		● 禘(40) ■ 中(197) ● (氏(20) ● 信息(2)		立即执行	¢	已完成	启动
资产对比 🔹 👻	1	225	> win8_50.202	WEB扫描 □令猜解 系统扫	描 172.20.50.202		● 商(3) ● 中(0) ●低(28) ●信息(12)● 弱口令(0)	立即执行	¢	已完成	启动
系统管理 >	1	224	> 数据库检测-172.20.50.2	01 数据库检测			●商(0) ●中(0) ●低(0) ●信息(0)		立即执行	÷	已完成	启动
		223	> 172.20.57.42深度扫描	WEB扫描【口令猜解】系统扫	描 172.20.57.42		●商(37) ●中(26) ●低(17) ●信息(5)	● 弱口令(0)	立即执行	¢	已完成	启动
		218	> 172.20.57.42标准扫描	WEB扫描 □令猜解 系统扫	描 172.20.57.42		●商(0) ●中(2) ●低(29) ●信息(3)	● 弱□令(0)	立即执行	中	已完成	启动
		217	> 172.20.57.42dcbox	WEB扫描 □令猜解 系统扫	描 172.20.57.42		● 裔(92) ● 中(65) ● 低(34) ● 信意(9)	● 鹅口令(0)	立即执行	÷	已完成	启动
		216	> 172.20.57.51	WEB扫描 □令猜解 系统扫	描 172.20.57.51		● 裔(128) ● 中(68) ●低(62) ●信息(16) - 弱口令(0)	立即执行	÷	已完成	启动
		215	> 172.20.52.230AS	WEB扫描	描 172.20.52.230		●商(124)●中(59) ●低(183)●信息(35)● 弱口令(0)	立即执行	低	已完成	启动
		214	> 172.20.52.230	系统扫描			●商(4) ●中(10) ●低(27) ●信息(13		立即执行	#	已完成	启动
		213	> 172 20 54 172	彩体扫描			● 奈(32) ● 中(63) ● 任(26) ● 信章(25		立即执行	#	已完成	

图 4.2.1.5-1 删除任务

4.2.1.6 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

复制任务		×
* 新任务名称 * 新扫描目标	172.20.54.246_copy 172.20.54.246	* 提示: 请填写任务名称,长度在[1-40]字符之间 * 扫描目标填写规范: IP示例: 192.168.1.100,2001:fecd:ba23:cd1f:dcb1:101 0:9234:4088 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.* 域名示例: www.example.com URL示例: http://192.168.1.100/,https://www.exampl e.com/,http://[2001:fecd:ba23:cd1f:dcb1:1010:9234:40 88]/ 排除IP或IP段: 1192.168.1.1/24,1192.168.1.1-255,1192.1 68.1.1 美似192.168.3.cc、192.168.bb.cc、192.aa.bb.cc格式将 会被视为域名,请确认后提交 多个之间以英文逗号(.)或换行分隔
提交		

图 4.2.1.6-1 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

任务 🔻	任务名称	扫描类型	扫描目标	检测结果	执行方式	优先级	任务状态	操作
231	> 172.20.54.246_copy	系统扫描	172.20.54.246	● 高(0) ● 中(0) ● 低(0) ● 信息(0)	立即执行	中	排队	停止

图 4.2.1.6-2 复制任务

4.2.1.7 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

	() BIR	1112月 / 二 12月1	18							
	• 6	王务列表	e 工作列表		Rithin	ng fallallance mail Mill x antico mail+	liw a	32	全部任务	* NR(53)
		(ESID	• E\$8#	白揚天堂	T198/ERA	检测热果	执行方式	优先摄	任命状态	股份
	2	13	> 日令債解全部172.20.54.1-172.20.54.255		172.20.54.1-172.20.54.255,1172.20.57.51	 ●第□⊕(741) 	立即执行		已完成	80
		12	> 172.20.54.1-172.20.54.255	WEBERN DOORS MARINE	17220541-1722054255/172205751	●資(3342)●中(5495)●臣(5542)●臣臣(1529)●問□⊕(739)	立即执行	ф	已完成	80
		11	> test IEIEIEIE	WERGIN DORM EMON	172,20,51,111,1172,20,57,51	●页(0) ●中(0) ●任(0) ●信息(0)●数□令(0)	2005/7	æ	已完成	R0
		10	> haha	WEINING DOMM BURNING	172.20.51.156(1172.20.57.51	●満(0) ●中(0) ●低(0) ●価度(0) ●第二中(0)	立即的行	- ep	ERM	RB
		9	> test1	WENTER DOME BRITER	172.20.57.39(172.20.57.13)(172.20.57.51)	■凝(18) ●中(40) ●低(116) ●依恕(26)●第□中(0)	立即执行		已完成	and the
		8	> 172.20,54.202	承诺扫描	172.20.54.202,1172.20.57.51	●潤(7) ●中(4) ●低(35) ●信息(25)	2月0847	-01	已完成	60
		7	> 数据库检测-172.20.57.50-172.20.57.100	對國際检測	172.20.57.50-172.20.57.100,1172.20.57.51	●満(0) ●中(0) ●低(0) ●低(0)	立即称行		已停止	展開
		6	> 172.20,54.116歲2日	WEBRIN RALISS	172,2054,116,1172,20,57,51	●潤(1) ●牛(3) ●低(27) ●信息(4)	立即称行	#	已完成	80
		5	> 172,20.51.111	8001088	172,20,51,111,1172,20,57,51	●潤(0) ●中(0) ●任(0) ●信服(0)	2月29月7	ф	已抱成	-
		14	> 172.20.66.14	WEDER SHEETSE	172.20.66.14/172.20.57.51	●満(10) ●中(19) ●低(42) ●債幣(12)	立即执行		已完成	R 10
		3	> 172.20.57.1-172.20.57.200	网络扫描	172.20.57,1-172.20.57,200,1172.20.57.51	●渡(897) ●中(1711)●低(847) ●領戀(618)	立即纳行	4	已完成	en.
		2	> 172.20.57.51	8.841318	172.20.57.51)172.20.57.51	●濁(0) ●中(0) ●低(0) ●低量(0)	230847		已停止	80
	息计12	isida								19787 3 1



	SECLEAD MENSION	漏洞扫描安	全评估报告		日录
				📑 砅 🔎	2 任冬尚休飘览
				u u u	21 仟名基本信目
1 检测	结果综述				2.2 敏感端口/服务
					2.3 敏感中间件
本次	次检测中,扫描了	1个主机,0个站点。		APP VIEW VIEW LL + A	3 资产信息统计
松田	则到潮洞共23个。	系统庵洞23个,Web馮洞0个。高卮潇洞共9个,甲卮馮洞共5个,	(比厄漏洞共5个, 信息	双满洞共4 个。	3.1 端口/服务统计
120					3.2 资产风险等级
2214	4.风险等级力 •	于市,尼州型 ,非常危险的资产共1个,需里点大注。			3.2.1 主机资产风险
112	台休期时				3.2.2 WEB资产风险
2 11 75	05040166503				4 漏洞信息统计
2.1 任务	务基本信息				4.1 支影明页广动计 4.1 1 系统漫词影响资产
1000000					4.1.2 WEB漏洞影响资产
任务名	3称	172.20.54.246			4.2 漏洞等级分布
扫描目	标	172.20.54.246			4.3 漏洞类别统计
报表栲	版	4.3.1 系统漏洞类别			
任务所	所在账号	admin			4.3.2 WEB漏洞类别
扫描的	间	系统扫描: 2023-05-08 14:48:42 至 2023-05-08 14:55:01 (#	師: 6分19秒)		4.4 週刊作名 4.4.1 系统演演TOP10
系统版	反本	V3.0(6.6.1-R1-v90757-20230222)			4.4.2 WEB漏洞TOP10
规则盾	版本	20230324144746			5 弱口令
2.2 敏!	感端口/服务				6 历史检测详情
本次	大任务检测到开放	【了以下【2】种敏感端口或服务,开放最多的端口为【80】端口,又	拉【1】个资产,具(4情况如下表所示。	7 参考标准 7.1 单一漏洞风险等级评定标准
序号	端口	服务	协议	主机	7.2 资产风险等级评定标准
1	80	vmware esxi server/http/VMware ESXi Server httpd	TCP	172.20.54.246	8 安全建议
2	443	https	TCP	172.20.54.246	9 #R##2013
说明 2.3 敏援	月:敏感端口/服约 感中间件	各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。			
本次	次任务检测到以下	《种敏感中间件,其中使用最多的中间件是【】,具体情况如下表所;	J 72		
序号	中间件	网站			
说明	月: 敏感中间件是	指安全研究表明,容易被黑客利用发起攻击的中间件。			
3 资产	信息统计				
3.1 端[口/服务统计				
资产	≃的端口/服务开放	效情况如下表所示,开放端口最多的资产为【172.20.54.246】,共	开放了【7】个靖口:		
÷0	+10.27				

图 4.2.1.7-1 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

享号	IP (域名)	高	中	低	信息	总计(次)
1	172.18.0.252	6	1	4	0	11



1 检测结果综述	
本次报告中,目标 整体风险值为6.6 准》)。	录【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。 ,安全等级为 <mark>9比较危险。</mark> 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
2 资产总体概览	
 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	\$2-053Demo
网站编码	UTF-8
服务器语言	
阿站物理地址	
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 海风脸:6 中风脸:1 任风脸:4 痕息:0
漏洞状态标识	新增:11 误报:0 已修复:0
密产组	zx-webscan

图 4.2.1.7-2 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 5 2 2 2,即可将任务报表导出到本地

4.2.2 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 5.2.2-1 所示:



 ● 系统监控 ○ 驗弱性管理 		 ● 任务列表 ■ 工作 	列表				局新こ 搬索[回车]	
新建任务		检测对象	▼ 任务名称	开始时间	检测耗时	进度	操作	
□ 任务管理		172.20.50.200	已有靶机扫描	2023-05-06 18:48:06	1天	漏洞数: 812 网页数: 4661 <u>剩余</u> 日	j词: 410.07分钟 停止■	
② 数据库检测		总计1条记录						< 1 >
② 安全基线检测								
103 资产管理								
壹 资产组管理								
亘 导出报表								
◎ 模板管理	×							
⊙ 资产对比	*							
⊙ 系统管理	×							

图 4.2.2-1 工作列表

工作列表各项参数说明如表 4.2.1-1 所示:

表 4.2.1-1 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。

4.3 数据库检查

WEBUI: 主界面 -> 任务中心 -> 数据库检查

4.3.1 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 4.3.1-1 所示:



會 系统监控	1.000								
◎ 脆弱性管理 ^	□ 数据库检测								
③ 新建任务	检测基本配置 登录信息选项	检测基本配置 豐汞信息造项 存活配置造项 探测造项 检测造项 目标选项							
10 (* 4* b* 10	扫描目标方式	日期目标方式 ④ 手动輸入 (使用波产) 批量导入							
目 任务管理									
② 数据库检测	扫描目标			* 输入的內容有單个无則以且表現面特, 多个之间以美文是专家就称分编 當个主批示例:192168.1100 也可使用城客: www.example.com IPv6示例: 3000000000000000000000000000000000000					
② 安全基线检测			,	※ 主規組元例: 192.168.1.0/24,192.168.2.1-254,192.168.3.1-192.168.3.254 期除P取P段P段: 192.168.1.1/24,192.168.1.1-255,192.168.1.1 第約193.168.2.cc					
四 资产管理				96以192.100.5.00、192.100.00.00、192.88.00.00世10号至彼位/3線点, 南明の山地文					
	任务名称	数据库检测-		* 提示: 请填写任务名称, 长度在[1-40]字符之间					
三 资产组管理	漏洞插件模板	数据库安全漏洞 *							
亘 导出报表	调试模式	×	若开启,则记录目标详细插件执行日志。						
⊙ 模板管理 ✓	执行方式	立即执行	*提示: 请选择执行方式						
⊙ 资产对比 ✓	分布式引擎	默认	默认:系统将根据引擎的负载情况,智能选择工作引擎。同	时也可以指定引擎					
⊙ 系统管理 ✓	执行优先级别	ф •	当任务达到并发上限时,"排队等待中级别魔的任务将优先执行。						
	告警模板	无	告警发送及接收设置,请到[系统管理>任务告警]下配置						
		提交							

图 4.3.1-1 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 4.3.1-1 所示:

参数	说明						
	1. 手动输入: 可输入单个主机或主机组,即扫描对象						
扫描目标方式	2. 使用资产: 扫描已知资产,资产管理界面需要有资产						
	3. 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 1. 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 2. 单个主机示例: 192.168.1.100 也可使用域名: www.example.com 3. IPv6示例: 2001:fecd:ba23:cd1f:dcb1:1010:9234:4088 4. 主机组示例: 192.168.1.0/24,192.168.2.1-254,192.168.3.1-192.168.3.254 5. 排除某个 IP: 192.168.1.0/24!192.168.1.100						
任务名称	可自定义,默认前缀是为了区分不同的扫描任务						
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						
调试模式	默认不记录扫描执行日志,若开启将记录扫描执行日志。						
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						
告警模板	告警发送及接收设置,请到[系统管理>任务告警]下配置						

表 4.3.1-1 配置参数说明

4.3.2 登录信息选择



可对扫描任务靶机进行登录验证。

B 關發性检測包	○ 旅游性松弛 / ▲ 教展中检測							
壹 任务管理	□ 数据库检测	□ 数据库检测						
▲ 数运作检测	检测基本配置 登录信息选项 存活配置选项	探测选项 检测选项	引擎选项					
a 安全基线检测						1	新增+ 批量验证C 刷新	
图 脑弱性资产	□ 目标地址	数据库	端口	用户名	慶码	操作	验证结果	
節 顧勞性资产组	没有检索到数据							
							* 3	
		冬	4.3.2-1	数据库扫	描-登录验证			

4.3.3 存活配置选项

可对扫描任务靶机进行存活验证。

□ 数据库检测		
检测基本配置 登录信息选项	存活配置选项 探测选项 检测选项 引擎选项	
发包速率	○ 快速 ○ 正常 ○ 慢速 ● 自适应 ○ 自定义	快速:单ip3000包/s 正常:1500包/s 優速:1000包/s 自定义:单个ip在100-5000包/s 范围
主机存活探测	×	如果关闭,则认为目标主机存活,直接进入端口扫描阶段
	✓ ARP	
	J ICMP PING	
	TCP PING 21,22,23,25,80,443,445,139,3389,61	
	UDP PING 25,53,161	
端口扫描范围	 ● 标准 ○ 快速 ○ 全部 ○ 指定 	标准: 默认講口2000多个。快速: 1000个常用調口。全部: 講口1-65535 指定: 単个或范围知22,1-1024,指定102時口: TCP:1024-65535,指定 UDP調口: UDP:1025-65535。 金点击下彀,了解講口详情。
TCP端口扫描方式	CONNECT SYN	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

图 4.3.3-2 数据库扫描-登录验证

数据库扫描-存活配置选项参数说明如表 4.3.4-1 所示:

参数	说明
发包速率	支持对发包速率的配置 1.快速:单 ip3000 包/s 2.正常:1500 包/s 3.慢速:1000 包/s 4.自定义:单个 ip 在 500-5000 包/s 范围
主机存活测试	对扫描主机的探测方式: ARP, ICMP PING, TCP PING, UDP PING ARP:通过 ARP 请求来实现探测,一般防火墙没法过滤 ARP 协议,成功率比 ICMP ping 高。 ICMP PING:测试网络的可达性和网络延迟。 TCP PING:使用 TCP 来向目标服务发送一个简单的 TCP 连接请求,等待服务器的响应。 通常用来测试服务器是否在线和网络延迟。



	UDP PING:使用 UDP 来向目标服务发送一个简单的 UDP 数据包,等待服务器的响应。 通常用来测试网络质量和服务端的响应时间。 默认四个都勾选
端口扫描范围	1. 标准: 默认端口 4000 多个。 2. 快速: 100 个常用端口。 3. 全部: 端口 0-65535 4. 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	1. CONNECT 方式为全连接扫描,完成 TCP/IP 的三次握手,速度较慢 2. 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

4.3.4 探测选项

□ 数据库检测	i				
检测基本配置	登录信息选项	存活配置选项	探测选项	检测选项	引擎选项
提示被扫目标		×	在打	3描之前提示被	扫描主机,需要扫描目标支持messager服务
			图 4	3 4-1 券	为据库扫描-探测洗项

数据库扫描-探测选项配置参数说明如表 4.3.4-1 所示:

表 4.3.4-1 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

4.3.5 检测选项

羚见数据安全检查工具箱用户手册



□ 数据库检测					
检测基本配置 登录信息选项	存活配置选项	探测选项	检测选项	引擎选项	
最大限度报告漏洞	1	若选	择开启: 扫描	結果中不是所有漏洞都经过原理扫描得出, 会有一些根据版本信息推测出来的漏洞	
执行所有规则检测	×	若选	择开启: 检测	则耗时越久、对检测目标的覆盖面更广	
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			
启用口令破解	×	使用	默认字典对系	系统或服务的口令进行猜解	
测试Oracle账号	×				

图 4.3.5-1 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 4.3.5-1 所示:

表 4.3.5-1 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							
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							
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							

4.3.6 引擎选项

□ 数据库检测			
检测基本配置 登录信息选项	存活配置选项 探测选	页 检测选项	引擎选项
插件超时 (秒)	30		单个插件执行时间最长设置[10-300]
单个主机检测并发数	5		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	500 🗘		单个扫描任务,可同时扫描的主机数量[1-500]
单个主机TCP连接数	45		针对单个检测目标,并发的TCP连接数量[1-1024]

图 4.3.6-1 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 4.3.6-1 所示:

表 4.3.6-1 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]
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]

4.4 安全基线检测

安全基线检测采用机器语言,模拟人访问 IT 资产的全过程,自动化的采集各 IT 资产的 安全配置,并对安全配置信息进行自动化解析,与安全知识库中的安全配置要求及基准点进 行比对,以检查安全配置符合情况,自动化出具丰富详实的核查报告。

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 5.4.1 所示:

能够性检测包	○ 照相性检测 / 4 安全基线检测							
任务管理	日 安全基线检测							
数据库检测	任务类型	 • 在线任务 ○ 高线任 	务					
安全基础检测	扫描目标方式	 手动输入 使用资 	☞ ○批	聖导入				
能弱性变产 能弱性变产相	扫描目标	172.20.54.172					* 输入的内容为单个主机, 多个之间以英文逗号 单个主机示例: 192.168.1.100 IPv6示例: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	,或换行分辐 occooox
	任务名称	基线核查-172.20.54.172				"	*提示: 请填写任务名称,长度在[1-40]字符之	(11)
	核查规范	默认安全配置规范	٠	* 提示: 扫描策略选择				
	设备信息	不使用跳板机	*	选择后该任务所有设备	的使用此跳板机【只支持	\$SSH协议】;如不选持	译,可针对每个设备单独设置跳板机。点击此处新	地统极机
		iPtété		登录协议	y Milli	0 用户名	配置模板	操作
		172.20.54.172		SSH	40000	root	Redhat/CentOS 7.x配置模板	编辑》
	目他配置选项 ~							
	执行方式	立即执行	٠	*提示:请选择执行方式	t			
	分布式引擎	BRIA	*	默认:系统将根据引擎	的负载情况,智能选择	工作引擎。同时也可以	指定引擎	
	执行优先级别	φ	*	当任务达到并发上限时	"排队等待中'级別高的	任务将优先执行。		
		~		若开启,则记录目标;	我细播件执行日志。			
	调试模式							

图 4.4 基线核查任务列表

4.4.1 在线任务-检测基本配置

新建在线的基线检测任务:针对在线检测任务,输入目标、任务名称,选择扫描策略, 配置登录信息和核查的模板类别并配置其他选项提交任务。如图 4.4.1 所示:



」關始性控制也	○ 新丽性检索 / α 安全基线检测		
1 任务管理	日 安全基线检测		
数泥库检测	任务类型	 在线任务 -	
安全基础检测	扫描目标方式	 • 手动输入 ○ 使用资产 ○ 批量导入 	
脱弱性资产 脱弱性资产机	扫播目标		* 输入的内容为除个主机。多个之间以负文道号。或换行分幅 单个主机切射: 192.168.1100 IP46页码: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
	任务名称	幕结检查-	 #示: 请填写任务名称,长度在[1-40]字符之间
	核查规范	默认安全配置规范 * "提示:扫描策略选择	
	设备信息	不使用能板机 * 选择后该任务所有设备均使用此跳板机【只支持SSH协议】;	;如不选择,可针对每个设备单独设置跳版机,点击此处新增融版机
		IP地址 登录协议 编口 用户	2名 配置模板 操作
	其他配置选项 ~		
	执行方式	立即执行 * "提示:请选择执行方式	
	分布式引擎	默认 * 默认:系统将根据引擎的负载情况,智能选择工作引擎。同时	时也可以指定引擎
			http
	执行优先级别	+	M).
	执行优先级别 调试模式	* 若汗島、剣记梁目病洋細語件执行日志。	ni je

图 4.4.1-1 新建基线核查任务

新建基线核查任务配置参数说明如表 4.4.1 所示:

参数 说明 1. 在线任务: 下发任务时配置好目标主机的登录信息, 系统远程访问进行检测 创建任务方式 2. 离线任务: 将离线模板下载到目标主机上, 在目标主机上检测完后后将结果导入系 统进行结果查询 手动输入:可输入单个主机或主机组 扫描目标方式 使用资产:扫描已知资产,需先在【资产管理】下添加 批量导入:以Excel的格式导入,减少工作量 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 检测目标 1. 单个主机示例: 192. 168. 1. 10 2. 主机组示例: 192. 168. 1. 1-192. 168. 1. 10 范围不超过 255 个 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

表 4.4.1 配置参数说明

●设备列表配置:设备列表用来展示并配置目标主机登录信息和选择检测模板,如下图 4.4.1-2



BEAALT4ESSIFE	② 肥利性检测 / 4 安全基线检测					
1 任务管理	日安全基线检测					
数据库检测	任务类型	 • 在线任务 ○ 高线任务 	5			
安全基线检测	扫描目标方式	 手动输入 使用资 	☆ ○ 批量导入			
能弱性资产 能弱性资产组	扫描目标	172.20.54,172			* 输入的内容为单个主机,多个之间以质立退号 单个主机示例: 192.168.1.100 IPv6示例: xxxxcxxxcxxxcxxxxcxxxxxxxxxxxxxxxxxxx	号,或换行分隔 0000000
	任务名称	基线核查-172.20.54.172		"	*提示: 请填写任务名称, 长度在[1-40]字符之	2[8]
	核查规范	默认安全配置规范	* 提示:扫描策略选择			
	设备信息	不使用跳板机	* 选择后该任务所有设备均	e用此跳板机【只支持SSH协议】;如不逮	封释,可针对每个设备单独设置跳板机,点击此处影	所謂與此被同初。
		IP地址	登录协议	▼ 端口 非 用户名	配置模板	操作
		IP地址 172.20.54.172	登录协议 SSH	▼ 篠口 非 用户名 40000 root	配置模板 Redhat/CentOS 7.x配置模板	操作
	其他武震违项 ~	IP地址 17220.54.172	登录协议 SSH	▼ 総口 用户名 40000 root	配置模板 Redhat/CentOS 7.x 在2 置接版	股作 SEZ
	其他武震进兵 ~ 执行方式	19地址 172.20.54.172 立即407	登录协议 SSH * "提示:请选择执行方式	★ 議口 目的容式 40000 root	能繁荣板 Redhat/CentOS 7.4在重转版	INTE ISSUE
	其他記憶原則 ~ 执行方式 分布式引擎	1722054.172 1722054.172 立即所行 2634		 ・ 第日本 ・ 第日本 ・ 1000 ・ 1000 ・ 100 ・ ・ ・	起軍機械 Redhat/CentOS 7.過2面機能 以過25回業	NA Ser
	其他此演派选择 ~ 执行方式 分布式引擎 执行优先规则	IP地址 1722054.172 立即地行 発い、 中	自动协议 SSH • 借示:请选择执行方式 • 默认:系统将把服司增约 • 部行先送则并发上期时, •		起国機械 Redhat/CentOS 7.20国際版 以指記当様	N/T See/
	其他此王国达明 ~ 执行方式 分布式引擎 执行优先规则 调武规式	iPitta 1722054.172 立即所了 批认 中 マ			起国機械 Redhat/CentOS 7.或国際版 以指記231章	NA Ser

图 4.4.1-2 设备列表

●设备列表生成方式有两种:

(1)手动输入或者导入, IP 地址由扫描目标自动生成, 点击操作栏的【编辑】手动配置目标主机登录信息和检测模板;如下图 4.4.1-3

编辑设备			×
基本属性			
设备地址	172.20.54.172		
登录协议	SSH 💌	协议端口	40000
登录账号	root	登录密码	
跳板机	不使用跳板机	登录验证	
设备模板 设备模板 su用户 数据库	Redhat/CentOS 7.x配置模板	su密码	
		新増模板	
应用服务器			
		新増模板	
确定取	肖		

图 4.4.1-3 编辑设备信息



(2)使用已检测过的资产,下拉选择历史任务和检测时间,直接继承旧任务的配置信息,如下图 3.4.1-4

Billio State Accession 198	③ 限制性检测 / 4 安全基线检测								
≟ 任务管理	田 安全基线检测								
▲ 数据库检测	任务类型	 • 在线任务 							
a 安全基线检测	扫描目标方式	● 手动输入 ④ 使用资产	○ 批量导/	~					
③ 胞弱性资产	使用资产	授索		× 172.20.54	.172	默认资产组	右边为已选资产。		
☐ #8894580×41		- 回 秋以微吟相 [1722.05.57.51] [1722.05.75.51] [1722.05.4.246] [1722.05.62.033] [2] 1722.05.4.172							
	历史配置引用	基线核查-172.20.54.172Baseline			*	(最近一次) 2023-12-12	2 15:13:17 至 2023-12-12 15:16:42		
	任务名称	基线核查-172.20.54.172			请选择历史时间				
	核查规范	默认安全配置规范	* *提	示: 扫描策略选择		(搬近一次) 2023-12-	-12 15:13:17 全 2023-12-12 15:10:42		
	设备信息	不使用跳板机	* 选择	后该任务所有设备均位	更用此跳板机【只支	寺SSH协议】;如不选持	¥,可针对每个设备单独设置跳板机。点击此处新	增跳板机	
		IP地址		登录协议	• 編口	0 用户名	配置模板	操作	
		172.20.54.172		SSH	40000	root	Redhat/CentOS 7.x配置模板	2001	
	目他配置洗項 ~								
	执行方式	立即执行	* * 提	示: 请选择执行方式					
	公本計21些	me+1	* Btil	: 系统编程图 11200	帝敬情况,智能洗择	工作引擎。 同时也可以将	「日本日間」		

图 4.4.1-4 选择历史配置信息

基线检测目标主机信息配置和模板选择参数说明如下表 4.4.1-2:

表 4.4.1-2 设备列表配置参数表

参数	说明
编辑设备	登录目标主机所需的协议、端口、账号、密码,目前支持协议有:SSH、Telnet、RDP、SMB、WinRM
设备模板	根据目标主机的操作系统、设备类型选择对应的设备模板
数据库配置模板	根据所选的设备模板,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:mysq1数据配置 /usr/bin/mysq1
应用服务器模板	根据所选的设备模板,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确,协议所选是否支持

4.4.2 离线任务-检测基本配置

离线任务:将在目标靶机上执行的基线核查结果导入到系统,直接进行解析和结果查看, 没有远程登录和检测的过程,创建离线任务如下图 4.4.2-1:



图 總弱性檢測包	C SENTERIA / ** STANDAR				
⇒ 任务管理	日安全基线检测				Î
▲ 数据库检测	任务类型	○ 在线任务 ● 离线任务			1
a 安全基线检测	任务名称	基线核查-172.20.54.172		*提示: 请填写任务名称,长度在[1-40]字符之间	- 1
記 脆弱性资产	核查规范	默认安全配置规范	 "提示:扫描策略选择 		- 1
龍弱性資产相	唐线结果		浏览 支持xml跟zip格式文件导入		- 1
	其他配置选项 ~				. 1
	调试模式	1 C	若开启,则记录目标详细插件执行日志。		- 1
	告醫模板	无	* 提示:告警发送配置,请到(系统管理>任务告鉴)下设置		- 1
		100-00-			- 1
					- 1
					- 1
					- 1
					- 1
					- 1
					- 1
					- 1
					- 1
					v

图 4.4.2-1 选择历史配置信息

离线任务配置参数说明见下表 4.4.2-1:

表 4.4.2-1; 离线任务配置参数表

参数	说明
创建任务方式	1. 在线任务: 下发任务时配置好目标主机的登录信息,系统远程访问进行检测 2. 离线任务:将离线模板下载到目标主机上,在目标主机上检测完后后将结果导入系统进行结果查询
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。
离线结果	将在目标靶机上执行的结果导入到系统,支持 zip 和 xml 格式,错误的文件无法解析

▲ 备注:目标靶机检测的模板需要在扫描策略里包含,若不包含,即使离线结果有数据,导入后 也无法解析

离线安全基线检查过程:

(1)选择离线任务后,输入任务名称,选择核查规范

(2)导入离线结果,离线结果支持 xml 或 zip 格式导入,最后选择所需要的告警模板

4.5 脆弱性资产

WEBUI: 主界面 -> 脆弱性检测-> 脆弱性资产

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 5.5-1 所示:



🎅 数据安全检	查工具箱系统		
肥弱性检测包	◎ 脑弱性检测 / 3 脑鞘性斑/*		
三 任务管理	◎ 资产管理		新增+ 批量令入主 号出主
▲ 数据连检测 		金師资产: 7 主机资产: 3 WEB资产: 4	
· 總弱性资产	全部字段 * 现来	操作系统 * mac地址	* 🛛 🕺 🏛
龍弱性資产相	▲ 资产 ♀	◇ ●资产属性	1949 · · ·
	□ ● 秋以第 ⁴ 纪 ■ http://112.94.70.96/ ■ http://112.94.70.96/ ■ 172.20.54.246[172.20.54.246] 任 172.20.54.246[172.20.54.246] 任 172.20.54.246:8000[172.20.54.246] 任 172.20.54.246:8000[172.20.54.246]	 PA込城会: 112.94.70.96 PAD込城会: gb2312 Ip地址: 112.94.70.96 物理地址: 「方面「州市-职題[112.94.00-11] 波产电型: WEB宽声 所面的干组: 数以宽声组 FK面的干组: 数以宽声组 	费/"网始值: 5.0 12.94.75.98]
		风险举情	▼高 ▼中 ▼低 ▼信息 限を測測名称
		风险等级 🔺 漏洞名称	漏洞所满分类 息计
		域名访问跟制不严格	A5 安全配置 1
		相反約 Form表单无CSRF保护	A8 跨站请求 32
		在风险 未禁用密码表单自动完成。性	A2 失效的身 6
		间接路 文件路径逻辑	A6 敏感信息 2 🐙

图 4.5-1 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。

4.5.1 系统资产

系统资产:展开资产树中的资产组,资产组下为资产名称,资产下为该资产的扫描任务, 系统资产下有系统扫描,数据库扫描,基线扫描,仅存活,口令猜解几种任务.如图 4.5.1-1

會 系统监控		2 WT 1818						
◎ 驗弱性管理	^					新增+ 批担	守 大王 (4)	11. 2
⑤ 新建任务				全部资产:	903 主机资产: 554 WEB资产: 349			
□ 任务管理		全部字段 v 搜索	操作系统		* maci <u>titit</u>	×	※ 董	
② 数据库检测								
② 安全基线检测		▲资产 田口 172.20.50.201:5357[172.20.50.201](admin)	~	● 资产属性				編編 个
KDS 资产管理		∏ 172.20.50.201:8750[172.20.50.201](admin) ∏ 172.20.50.201](admin)		● 风险详情		☑高 ☑中 ☑低	✔ 信息 控索局	名称
- 资产组装理				风险等级	漏洞名称		漏洞所属分类	总计
		[+] □ 172.20.57.51:2505[172.20.57.51](admin) [+] □ 172.20.57.51:9901[172.20.57.51](admin)		高风殿	检测到winrm登录存在弱口令【原理扫描】		默认探测	1
三 导出报表				高风险	Oracle Database Server Java VM组件代码执行漏洞(CVE-2014-6453)		其它	1
⊙ 模板管理	×	H□ 172.20.57.42[172.20.57.42](admin) □ 172.20.57.42[172.20.57.42](admin) □ 172.20.57.42](admin) □ 172.20.57.		高风险	PHP资源系统任意代码执行漏洞(CVE-2007-1581)		代码注入	1
⊙ 资产对比	~			高风险	Oracle Database Server Java VM组件安全漏洞 (CVE-2018-3110)		访问控制	1
◎ 系统管理	*	[+] □ 172.20.50.202:5985[172.20.50.202](admin) [+] □ 172.20.50.202:47001[172.20.50.202](admin)		高风险	Apache HTTP Server 缓冲区错误漏洞(CVE-2021-39275)		缓冲区溢出	3
		 172.20.50.203[172.20.50.203](admin) 系統扫描]172.20.50.203 		高风設	PHP 'exif process IED in JPEG' 函数安全漏洞 (CVE-2016-4543)		缓冲区溢出	1
		 ■ [□令猜解]172.20.50.203 ■ [基线核查]基线核查-172.20.50.203 		高限給	PHP (mmmt generic) 函数整数运出漂温 (CVF_2016_5769)		数字错误	1
		■ [数据库扫描]数据库检测-172.20.50.203		*5356			200 m 1 m 100	
					PRP mostings water water and (CVC-2000-5557)		地(王)(四)	
				高风险	PHP crypt函数缓冲区错误漏洞(CVE-2011-3268)		缓冲区溢出	1
				高风险	PHP WDDX扩展缓冲区错误漏洞(CVE-2016-3141)		缓冲区溢出	1
		□ 172.20.50.203:5985[172.20.50.203](admin)		高风险	PHP 'bcpowmod' 函数安全漏洞 (CVE-2016-4538)		输入验证	1
		(admin) (admin) (admin) (admin) (admin)		高风险	PHP 'exif_process_IFD_TAG' 函数安全漏洞 (CVE-2016-4542)		缓冲区溢出	1
				高风险	PHP 'wddx_deserialize()' 拒绝服务漏洞 (CVE-2016-7129)		输入验证	1
			- 1	高风险	phpMyAdmin SQL注入漏洞 (CVE-2019-11768)		SQL注入	1
		100 470 00 E0 000.0000[470 00 E0 000]/wdmin)	*	高风殿	Apache httpd 安全漏洞(CVE-2017-3167)		授权问题	1
				高风险	PHP 安全馬洞 (CVE-2017-8923)		缓冲区溢出	3

图 4.5.1-1 资产管理



▶风险详情

展示了所选资产最后一次检测时间段的检测结果

			全部资产	:	03 主机资产: 554 WEB资产: 349		
字段	▼ 搜索	操作系统			マ mact线社 マ	⇒ ₫	前重
产 🕜		~ 4	资产属性				编辑
±□17: ±□17:	2.20.50.201:5357[172.20.50.201](admin) 2.20.50.201:8750[172.20.50.201](admin)	1	风险详情		マ高 マ中 マ低	✔ 信息 搜索源	詞名称
+ [] 17: + [] 17:	2.20.50.201:47001[172.20.50.201](admin) 2.20.57.51[172.20.57.51](admin)		风险等级	▲ 3	用名称	漏洞所属分类	总计
+ C 17: + C 17:	2.20.57.51:2505[172.20.57.51](admin) 2.20.57.51:9901[172.20.57.51](admin)		高风脸	ŧ	金则到winrm登录存在弱□令【原理归描】	默认探测	1
E 🗆 17: E 🗆 17:	2.20.57.51:9910[172.20.57.51](admin) 2.20.57.51:9999[172.20.57.51](admin)		高风脸	C	Dracle Database Server Java VM组件代码执行漏洞(CVE-2014-6453)	其它	1
E 🗆 17: E 🗆 17:	2.20.57.42[172.20.57.42](admin) 2.20.57.42:2505[172.20.57.42](admin)		高风脸	P	HP 資源系统任意代码执行漏洞(CVE-2007-1581)	代码注入	1
0 17	2.20.50.202:5357[172.20.50.202](admin) 2.20.50.202:5985[172.20.50.202](admin)		高风脸	C	Dracle Database Server Java VM组件安全濡润(CVE-2018-3110)	访问控制	1
0 17	2.20.50.202:47001[172.20.50.202](admin) 2.20.50.203[172.20.50.203](admin)		高风脸	A	spache HTTP Server 缓冲区错误漏洞(CVE-2021-39275)	缓冲区溢出	3
	[系统扫描]172.20.50.203 [□会猜解]172.20.50.203		高风脸	P	'HP 'exif_process_IFD_in_JPEG' 函数安全漏洞 (CVE-2016-4543)	缓冲区溢出	1
	[基线核查]基线核查-172.20.50.203 [数据库扫描]数据库绘测-172.20.50.203		高风脸	P	HP 'mcrypt_generic' 函数整数溢出漏洞 (CVE-2016-5769)	数字错误	1
E C 17	2.20.50.203[172.20.50.203](admin)		高风脸	P	HP mbstring扩展缓冲区溢出漏洞(CVE-2008-5557)	缓冲区溢出	1
E 0 17:	2.20.50.203:5357[172.20.50.203](admin)		高风脸	P	HP crypt函数缓冲区错误漏洞(CVE-2011-3268)	缓冲区溢出	1
E C 17.	2.20.50.203:5466[172.20.50.203](admin) 2.20.50.203:5500[172.20.50.203](admin)		高风脸	P	HP WDDX扩展缓冲区描误漏洞(CVE-2016-3141)	缓冲区溢出	1
E C 17:	2.20.50.203:567/[172.20.50.203](admin) 2.20.50.203:5985[172.20.50.203](admin)		高风脸	P	'HP 'bcpowmod' 函数安全漏洞 (CVE-2016-4538)	输入验证	1
HU17: HU17:	2.20.50.203:7756[172.20.50.203](admin) 2.20.50.203:8000[172.20.50.203](admin)		高风脸	P	HP 'exif_process_IFD_TAG' 函数安全漏洞 (CVE-2016-4542)	缓冲区溢出	1
H 🗆 17: H 🗆 17:	2.20.50.203:8080[172.20.50.203](admin) 2.20.50.203:8085[172.20.50.203](admin)		高风脸	P	HP 'wddx_deserialize()' 拒绝服务漏洞 (CVE-2016-7129)	输入验证	1
E 🗆 17: E 🗆 17:	2.20.50.203:8088[172.20.50.203](admin) 2.20.50.203:8090[172.20.50.203](admin)		高风脸	p	hpMyAdmin SQL注入漏洞(CVE-2019-11768)	SQL注入	1
	1 20 E0 202-00021172 20 E0 2021/2dmin)	•	高风脸	A	Apache httpd 安全漏洞(CVE-2017-3167)	授权问题	1
			高风脸	P	HP 安全漏洞 (CVE-2017-8923)	缓冲区溢出	3

		全部资产: 903	主机资产: 554	WEB资产	5: 349			
鄂字段 v 邊愛	操作系统			mac地址			*	查询 重
夏产 🛛	\sim	● 资产属性						
+ 172.20.50.202:5985[172.20.50.202](admin)	*	● 风险详情						
⊞ □ 172.20.50.202:47001[172.20.50.202](admin) ⊡ □ 172.20.50.203[172.20.50.203](admin)		服务		▲ 端口		用户名	密码 ☞	
 ■ [系统扫描]172.20.50.203 ■ [□令猜解]172.20.50.203 		smb		445		Administrator	*****	
 ■ [#800/82] #80/82 11/2.20.50.203 ■ [#800/82] #80/82 11/2.20.50.203] (admin) ■ 172.20.50.203 [172.20.50.203] (admin) ■ 172.20.50.203 [172.20.50.203] (admin) ■ 172.20.50.203 [577 [172.20.50.203] (admin) ■ 172.20.50.203 [577 [172.20.50.203] (admin) ■ 172.20.50.203 [5677 [172.20.50.203] (admin) ■ 172.20.50.203 [507 [172.20.50.203] (admin) ■ 172.20.50.203 [500 [172.20.50.203] (admin) ■ 172.20.50.203 [8000 [172.20.50.203] (admin) ■ 172.20.50.203 [8000 [172.20.50.203] (admin) ■ 172.20.50.203 [8009 [172.20.50.203] (admin) ■ 172.20.50.203 [877 [172.20.50.203] [admin) ■ 172.20.50.204 [172.20.50.203] [admin) ■ 172.20.50.204 [172.20.50.204] [admin) ■ [164 ##] 172.20.50.204 [4 min) ■ [164 ##] 172.20.50.204 [172.20.50.204] ■ [164 ##] 172.20.50.204 [admin) ■ [164 ##] 172.20.50.204 [admin) ■ [164 ##] 172.20.50.204 [admin) 		总计1条记录						<u>с</u> 1

图 4.5.1-3 口令猜解--风险详情



 								新增+ 批量	导入土	导出土
		全部资产:	903	主机资产:	554	WEB资产:	349			
全部字段 * 搜索	操作系统	i e n			¥	mac地址		•	*	前重置
▲资产 ♀	\sim	● 资产属性								编辑へ
H □ 172.20.50.201:5357[172.20.50.201](admin) H □ 172.20.50.201:8750[172.20.50.201](admin)	^	● 风险详情						☑高 ☑中 ☑低	✔ 信息 搜索	层洞名称
		风险等级 🔺	漏洞名称						漏洞所属分类	总计
[] 172.20.57.51:2505[172.20.57.51](admin) [] 172.20.57.51:9901[172.20.57.51](admin) []		高风险	Oracle Da	atabase Serv	er Java VM组	件安全漏洞 (C\	VE-2018-3110)		访问控制	1
[□ 172.20.57.51:9910[172.20.57.51](admin) [□ 172.20.57.51:9999[172.20.57.51](admin)		高风险	Oracle Da	atabase SQL	主入漏洞 (CV	E-2005-0297)			SQL注入	1
		高风险	Oracle Da	atabase Serv	er Java VM组	件代码执行漏洞	(CVE-2014-6453)		其它	1
		高风险	Oracle Da	atabase Serv	er Java VM组	件代码执行漏洞	(CVE-2014-6467)		其它	1
		高风险	Oracle Da	atabase Serv	er JPublisher	组件代码执行漏	洞 (CVE-2014-6546))	其它	1
 ▶ [系统扫描]172.20.50.203 ▶ [□令猜解]172.20.50.203 		高风险	Oracle Da	atabase Serv	er Java VM组	件安全漏洞 (C\	VE-2015-0457)		其它	1
 ■ [基线核查]基线核查-172.20.50.203 ■ [数据库扫描]数据库检测-172.20.50.203 		高风险	Oracle Da	atabase Serv	er OJVM组件	本地安全漏洞(CVE-2016-5555)		其它	1
		高风险	Oracle Da	atabase Serv	er SQLJ组件代	、码执行漏洞(C	CVE-2014-6455)		其它	1
⊕ □ 172.20.50.203:5357[172.20.50.203](admin) ⊕ □ 172.20.50.203:5466[172.20.50.203](admin)		高风险	Oracle Da	atabase Serv	er Java VM组	件代码执行漏洞	(CVE-2014-6545)		其它	1
		高风险	Oracle Da	atabase Serv	er Java VM组	件安全漏洞 (C\	VE-2016-0499)		其它	1
		高风险	Oracle Da	atabase Serv	er Java VM组	件任意代码执行	漏洞 (CVE-2015-262	29)	其它	1
		高风险	Oracle Da	atabase Serv	er Java VM组	件安全漏洞 (C\	VE-2018-3259)		其它	1
		高风险	Oracle Da	atabase Serv	er Java VM组	件代码执行漏洞	(CVE-2014-6560)		其它	1
	-	高风险	Oracle Da	atabase Serv	er Core RDB	/IS组件任意代码	融行漏洞(CVE-2014	4-6567)	其它	1
		高风险	Oracle Da	atabase Serv	er Portable C	lusterware组件	安全漏洞 (CVE-2015	i-4863)	其它	1
		高风险	Oracle Da	atabase Serv	er Java VM组	件安全漏洞 (CN	VE-2015-4794)		其它	1

图 4.5.1-4 数据库扫描--风险详情

		全部资产: 903	主机资产: 554	WEB资产:	349			
部字段 ▼ 提滚	操作系统		¥	mac地址		٣	⇒ 1	询 重調
资产 📀	\sim (▶ 资产属性						
⊞□ 172.20.50.201:5357[172.20.50.201](admin)	A 9	▶ 风险详情						
T □ 172.20.50.201:8750[172.20.50.201](admin) 172.20.50.201:47001[172.20.50.201](admin)		模板名称						
		□ Win7/Windows Se	rver 2008配置模板					
						≤合规	☑ 不合规 ☑ 失败	☑人工判
		类别	风险级别	相	这查项名称		核查结果	
H □ 172.20.57.42[172.20.57.42](admin) H □ 172.20.57.42:2505[172.20.57.42](admin)		帐号管理	信息	枪	全重是否已删除或禁用帐户		不合规	
H □ 172.20.50.202:5357[172.20.50.202](admin) U □ 172.20.50.202:5985[172.20.50.202](admin)		□令策略	中风脸	枯	全是否已启用密码复杂性要求		不合规	
H □ 172.20.50.202:47001[172.20.50.202](admin) □ 172.20.50.203[172.20.50.203](admin)			中风险	杜	全重是否已正确配置密码长度最小值		不合规	
 ▶ [系统扫描]172.20.50.203 ▶ [□令猜解]172.20.50.203 			信息	枝	全是否已正确配置"强制密码历史"		不合规	
■ [基线核查]基线核查-172.20.50.203 ■ [数据库扫描]数据库检测-172.20.50.203			信息	枯	金星否已正确配置密码最短使用期限		不合规	
			信息	杜	全是否已正确配置帐户锁定时间		不合规	
			信息	枪	金是否已正确配置"复位帐户锁定计数	收器"时间	不合规	
			信息	枯	金是否已正确配置帐户锁定阈值		合规	
			信息	杜	全主是否已更改管理员帐户名称		不合规	
H □ 172.20.50.203: 7756[172.20.50.203](admin) D 172.20.50.203:8000[172.20.50.203](admin)			信息	杜	全要是否已正确配置密码最长使用期限		合规	
H □ 172.20.50.203:8080[172.20.50.203](admin) □ 172.20.50.203:8085[172.20.50.203](admin) □ 172.20.50.203:8088[172.20.50.203](admin)	- 11	总计63条记录			a	页显示 10 *	« < 1 2 3	4 5 >
+ 172.20.50.203:8090[172.20.50.203](admin)	-							

图 4.5.1-5 基线核查--风险详情

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 4.5-2 所示:

全部字段 ¥ 搜索	攝作系统 …	* mac找社	¥	≫ 直询 1
▲ 资产 0	◇ ●资产属性			编辑
 ➡ 172.18.253.88-172.18.253.255 ➡ 172.18.253.88 ➡ 172.18.253.186 	↑ 主机名称:	TEST-FREE		资产风险值:9.9
 ■ [系統扫描]172.18.253.186 ■ [□令猜解]172.18.253.186555 ■ [軟爆素扫描]軟爆素控制,172.18.253.186 	ip地址:	172.18.253.186		
	mac地址:	00:0c:29:b1:f3:fc		
□ 172.18.253.88 ■ [基线核查]基线核查-172.18.253.88	/編作差3%: 袖□:	Windows / Ultimate /601 Service Pack 1 23.80.135 音音全部		
	资产类型:	系统资产		
□ 172.18.0.173 ■ □ 172.18.0.173 ■ □ □ 172.18.0.173	所属资产组:	172.18.253.88-172.18.253.255		
	所雇用户:	yangjing		
H □ https://172.18.0.252/[172.18.0.252] 1	标签:			
	● 风险详情			€ ✓ 信息 捜索漏洞名称

图 4.5-2 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 4.5.2 Web 资产

Web 资产:展开资产树中的资产组,选择 web 资产, web 资产下为 web 扫描任务

≻Web 风险详情

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 5.5.2-1 所示:

❷ 资产管理								新增十	北星导入土	寻出 土
		全部资产:	903 主机资产:	554	WEB资产:	349				
全部字段 v 搜索	操作系统				mac地址			×	×	
蛊资产 €	~ •	资产属性								编辑 >
	•	网站域名:		1	72.20.50.204				资产风险	值: 9.3
H □ 172.20.50.202:5985[172.20.50.202](admin) H □ 172.20.50.202:47001[172.20.50.202](admin)		网页编码:		ß	SO <mark>-8859-1</mark>					
∃ □ 172.20.50.203[172.20.50.203](admin) ∃ □ 172.20.50.203[172.20.50.203](admin)		ip地址:		1	72.20.50.204					
H □ 172.20.50.203[172.20.50.203](admin) T □ 172.20.50.203:5357[172.20.50.203](admin) □ 172.20.50.203:E466[172.20.50.203](admin)		服务器语言:		P	HP/4.1.2					
		物理地址:		尼	影域网-对方和您在	司—内部网[172.1	16.0.0-172.31.255.255			
		服労譜信息: 図站振覧・		P	pache/1.3.24 (W	ect	dev			
H □ 172.20.50.203:8000[172.20.50.203](admin) □ 172.20.50.203:8080[172.20.50.203](admin)		资产类型:		v	VEB资产					
H □ 172.20.50.203:8085[172.20.50.203](admin) T □ 172.20.50.203:8088[172.20.50.203](admin) T □ 172.20.50.203:8090[172.20.50.203](admin) T □ 172.20.50.203.8090[172.20.50.203](admin)		所属资产组:		H	状认资产组					
		标签:								
		风险详情						高 🗹 中 🗹 🕼	モン 信息 捜索調	調名称
H □ 172.20.57.42:2505[172.20.57.42](admin) □ 172.20.50.204[172.20.50.204](admin) □ 172.20.50.204[172.20.50.204](admin) □ 172.20.50.204[172.20.50.204]		风险等级 🔺	漏洞名称						漏洞所属分类	总计
■ [二今猜解]172.20.50.204×p		高风险	跨站脚本攻击漏洞(编码	3)					A3 跨站脚	1
 □ 172.20.50.204[172.20.50.204](admin) ■ [Web扫描]172.20.50.204xp 		高风险	链接注入						A3 跨站脚	1
		高风险	框架钓鱼						A1 注入	1
		中风脸	启用了目录列表						A6 敏感信	42
		中风脸	域名访问限制不严格						A5 安全配	1



风险级别	高风险	
概要	目标存在跨始 1.跨站脚本攻 2.跨站脚本攻 用户浏览该页 危害: 1.恶意用户可 2.恶意用户可 息目的。	調本攻击。 活就是指恶意攻击者向网页中插入一段恶意代码,当用户浏览该网页时,嵌入到网页中的恶意代码就会被执行。 击漏洞,英文名称Cross Site Scripting,简称CSS又叫XSS。它指的是恶意攻击者向Web页面中插入一段恶意代码, 顶时,嵌入到Web页面中的恶意代码就会被执行,从而达到恶意攻击者的特殊目的。 以使用该漏洞来盗取用户账户信息、模拟其他用户身份登录,更甚至可以修改网页呈现给其他用户的内容。 以使用JavaScript、VBScript、ActiveX、HTML语言甚至Flash应用的漏洞来进行攻击,从而来达到获取其他的用户
解决方法	建议过滤用户	输入的数据,切记用户的所有输入都要认为是不安全的。
扫描详情		
	漏洞URL	http://172.20.50.204/index.php?appservlang=th
	问题参数	appservlang
	测试用例	GET /index.php?appservlang=th%22%3E%3Ca+href%3D%26%23106%26%2397%26%23118%26%2397%26%23115%26%2399%26%23114%26%23105%26%23112%26%23116%26%2358%26%2397%26%2310 8%26%23101%26%23114%26%23116%26%2340%26%2349%26%2341%3E201308151610%3C%2Fa%3E HTTP/1.1 Accept: */* Referer: http://172.20.50.204/ Host: 172.20.50.204 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	参数值后缀"> <a href="javascript:al<br">ert(1)>201308151610 ,服务端能够原样反射,建议在代码中加入对参数 中包含的&#等特殊符号的判断。</td></tr><tr><td></td><td>操作</td><td>浏览器验证♀ 通用验证● SQL注入验证▲</td></tr><tr><td></td><td>漏洞状态</td><td></td></tr></tbody></table>

图 4.5.2-1 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 4.5.2-2 所示:



♀ 资产管理						ŝ	稽+	批量导入土	●日本
	全部资产:	903	主机资产: 554	WEB资产:	349				
全部字段 * 搜索	操作系统		×	mac地址	()		¥		
▲ 资产 ②	◇ ● 资产属性								编辑
 ■ 172.20.57.42[172.20.57.42](admin) ■ 172.20.57.42:2505[172.20.57.42](admin) ■ 172.20.50.202:5357[172.20.50.202](admin) 	▲ 网站域名:		1	72.20.50.204					资产风险值: 9.3
	网页编码:		IS	0-8859-1					
	ip地址:		1	72.20.50.204					
	服务器语言		P	HP/4.1.2					
	物理地址:		尾	;城网-对方和您在	同一内部网[172.16.0.	0-172.31.255.255]			
	服务器信息		A	pache/1.3.24 (W	in32) PHP/4.1.3-dev				
	网站标题:		A	ppServOpenProj	iect				
	资产类型:		V	VEB资产					
H □ 172.20.50.203:8088[172.20.50.203](admin) U □ 172.20.50.203:8090[172.20.50.203](admin)	所属资产组		R	认资产组					
田 172.20.50.203:8093[172.20.50.203](admin) 田 172.20.50.203:8282[172.20.50.203](admin)	标签:								
	● 风险详情					》 间	✓ 中	✔低 ✔信	包 搜索漏洞名称

图 4.5.2-2 Web 资产管理-资产属性信息

4.5.3 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,完成后点击【提交】按钮即可。具体详情如图 4.5.3-1 所示:

资产目标		* 请填写资产目标,多个资产以逗号分隔。 主机资产填写示例:192.168.1.1, www.baidu.com web资产填写示例:http://www.baidu.com/
标签	添加一个标签	提示:输入标签后按回车确定
	提交	

图 4.5.3-1 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、ur1、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,如图 4.5.3-2



X

请选择需要上传的文件

导入excel

选择文件 支持.xls格式] asset_v…late.xls ℃	▲点击下载样例模	板, 了解格式约定
标签	产品部 🗙		
土上传	⊘重置		

图 4.5.3-2 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

4.5.4 删除资产

用户可以对资产进行删除,可删除整个资产组。具体详细信息如图 4.5.4-1:

能弱性检测包	◎ 重新性核素 / 13 胞腺性素素				
◎ 任务管理	◎ 资产管理			新版 × 新聞 + 月	北星导入主 写出主
▲ 数据序检测 ○ 安全基级检测		全部资产: 8	主机资产: 🚺 WEB资产: 🜗		
D MERITERA	全部宁段 * 授家	操作系统	* maci的社	*	⇒ 市询 正置
D 胞弱性资产组	▲资产 ♀	◇ ● 资产属性			编组
	□ ■ ● 172.20.54.202] □ 172.20.54.202] □ https://112.94.70.96/[112.44.70.96] □ 172.20.54.20172.20.57.51] □ 172.20.54.246[172.20.57.51] □ 172.20.54.246[172.20.54.246] □ 172.20.54.246[172.20.54.246] □ 172.20.54.246[3000][72.20.54.246] □ 172.20.54.246[3000][72.20.54.246] □ □ 172.20.54.246[3000]	资产失型:: 所属因产组: 所属用户: 标签:	系统的" 就认为"明 admin admin		

图 4.5.4-1 Web 资产管理-删除资产

4.5.5 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



或名	172.20.50.204	
网站标题	AppServOpenProject	
网站编码	ISO-8859-1	
提交		

主机名称	XL	
操作系统	Windows XP	
mac地址	00:0c:29:2c:38:31	

图 4.5.5-1 编辑系统资产属性

4.5.6 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

♀ 资产管理								删除 ×	新增+	批星导入土 导出土	
				全部资产: 903	主机资产: 554	WEB资产:	349				
全部字段	/ 證書:		操作系统		¥.	mac地址			¥	余 <u></u> 查询	重置
资产组		¥	标签	请选择标签		评分		۰.	- ¥		



2) 配置不同查询参数->点击查询,查看符合条件的资产信息



3 资产管理						删除 ×	新增+	批量导入土 导出土
			全部资产: 903 主机多	隆产: 554	WEB资产: 349			
全部字段 *	搜索	操作系统		٣	mac地址		*	☆ 査询 重置
全部字段		10.00	1022/T+477+ TM AN) (平公			
IP		(1)(日	请选择标签		H75 - Y			
URL 网站信息		~ •	资产属性					──────────────────────────────────────
网页编码 网站语言	.57.42[172.20.57.42](admin) .57.42:2505[172.20.57.42](admin)	•	主机名称:		XL			※本团险值·100
网站物理地址 田 □ 172.2	0.50.202:5357[172.20.50.202](admin) 0.50.202:5985[172.20.50.202](admin) 0.50.202:47001[172.20.50.202](admin)		ip地址:		172.20.50.204			
	0.50.203[172.20.50.203](admin) 0.50.203[172.20.50.203](admin)		mac地址:		00:0c:29:2c:38:31			
∃□172.2 ∃□172.2	0.50.203[172.20.50.203](admin) 0.50.203:5357[172.20.50.203](admin)		操作系统:		Windows XP			
	0.50.203:5466[172.20.50.203](admin) 0.50.203:5500[172.20.50.203](admin)		端□:		80,135,137 查看全部			
	0.50.203:5677[172.20.50.203](admin)		1-1-14 TH					

图 4.5.6-2 资产搜索

查询条件参数说明:如下表

表 4.5.6-1 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。

4.5.7 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



♀ 资产管理	_								删除×		新增+	批星导入土	导出土
			全部资产: 903	主机资产:	554	WEB资产:	349						
全部字段	▼ 搜索	操作系统			Ŧ	mac地址							☆ 査询 重置
资产组	····· *	标签	请选择标签			评分	2	×	÷	a.	٣		
▲资产 0		\sim	资产属性										编辑
 	.20.57.42[172.20.57.42](admin) .20.57.42:2505[172.20.57.42](admin) .20.50.202:5357[172.20.50.202](admin)	•	主机名称:		x	L							资产风险值: 10.0
∃ □ 172	20.50.202:5985[172.20.50.202](admin)		ip地址:		1	72.20.50.204							
± □ 172 ± □ 172	2.20.50.203[172.20.50.203](admin)		mac地 <u>址</u> :		0	0:0c:29:2c:38:31							
王 田 日 172	.20.50.203[172.20.50.203](admin)		操作系统:		V	/indows XP							
±□172	.20.50.203:5466[172.20.50.203](admin) .20.50.203:5500[172.20.50.203](admin)		端□:		8	0,135,137 查看:	全部						
⊞ □ 172 ⊞ □ 172	.20.50.203:5677[172.20.50.203](admin)		资产类型:		M	统资产							

1	А	В	
1	资产组名称	资产	
2	192.168.5.1	192.168.5.1[192.168.5.1]	
3		192.168.5.1[192.168.5.1]	
4	新增测试组	172.20.50.199[172.20.50.199]	
5		172.20.50.199[172.20.50.199]	
6	test		
7	默认资产组	172.20.52.115	
8			
9			
10			

图 4.5.7-1 资产导出

4.6 脆弱性资产组

WEBUI: 主界面 -> 脆弱性检测->脆弱性资产组

资产组管理模块 dcbox 用户具有该功能模块的操作权限。都可对该模块功能进行操作管理。dcbox 用户可以对所有用户的资产组进行操作,普通用户只能查看并操作自己的资产组。 用户可以根据自身资产系统的组织结构或者网络拓扑通过资产组对其进行分类分组

4.6.1 新增资产组

操作: 在脆弱性资产组页面->点击【新增】->输入资产组名称->点击提交



羚见数据安全检查工具箱用户手册

 畲 系统监控 >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	9 资产组制	管理			新增+ 局新2 搜索(回车)
⑤ 新建任务		5产组名称 🔻	资产范围	所腐用户	备注
□ 任务管理	□ 19	92.168.5.1	192.168.5.1	admin	192.168.5.1
② 数据库检测	- 8	f 增测试组	172.20.50.199	admin	靶机资产
② 安全基线检测	🗌 te	est	193.0.0.2	admin	
10 资产管理	□ ¥	机资产组	0.0.0.0/0	默认资产组	
壹 资产组管理	总计4条记录				每页显示 25 * 〈 1 〉
亘 导出报表					
 · 模板管理 · · ·					
⊙ 资产对比 、					
 ○ 系统管理 × 					
新增资产组					×
资产组名称				*提示: 请填写资产组名称	
资产组范围				* 范围填写规范: IPv4示例: 192.168.1.100,IPv6 IP段示例: 192.168.1.0/24,192 域名示例: www.example.com URL示例: http://192.168.1.0/24/1 排除某个IP: 192.168.1.0/24/1 类似192.168.3.cc、192.168,b/ 多个之间以英文逗号()或换行分	示例: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
备注		提交		提示: 资产组备注	

图 4.6.1-1 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

4.6.2 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, 删除资产组该资产组下的资产全部划分到默认资产组下,资产管理和资产资产组管理都没有 该资产组。

🕨 数据安全格	查工具箱系统				
8		副性相較 上流最好的 〇枚時代的 〇合規約會 〇	18340 《 166 21		
)最弱性检测包	◎ 胞的性检测 / ▶ 胞粉性的>>组				
任务管理	◎ 资产组管理			1960× 1880× 1680+ 588	io 服素(回车)
数据连检测	一 资产组名称	* 资产和用	新羅用户	8/1	
安全基场检测			admin		
胞弱性资产	□ 默认资产组		默认资产组		
脆弱性资产组	(1)+2年(7)日				每页目示 25 * (1)
		确定删除所选资产	图?	×	
				4001	



图 4.6.2-1 删除资产组

4.6.3 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 4.6.3 所示

苦たわら	**	· 度左(1,16)之间		
臭怓名称	test " Th	近往[4-10]之1月		
查询条件	× Win 8配置模板			
	查询 重置			
己选模板	暂时没有选择筛选条件			
	模板类别		核查项数量	
	Resin 4.x For Windows配置模板		5	
	Resin 4.x for Linux/Unix配置模板		6	
	Storm配置模板		7	
	WebSphere 7.x for Windows配置模核	反	8	
	TongWeb for windows配置模板		9	
	Nginx for Windows配置模板		9	
	TongWeb for Linux/Unix配置模板		9	
	Nginx for Linux/Unix配置模板		10	
	Jboss for Windows 配置模板		10	
	Jboss for Unix/Linux配置模板		10	
	总计99条记录			« < 1 2 3 4 5 >

图 4.6.3 新建基线策略

4.6.4 基线离线模板

基线离线模板可以提供用户下载,远程对主机进行扫描生成离线结果



▲北市船侯仮 ▲ 基北南北侯仮			
■ 模板类別	◇ ○ ▲配置模板	◇ ○ ▲ 检查项列表	
模板类别	⇒ 模板名称	▲ 編号 ≑ 名称	
全部	AIX7.1配置模板	1 检查是否设置口令失效提示	
主机	Debian 5.x/7.x配置模板	2 检查是否禁用root用户远程ssh	
数据库	Debian 8.x配置模板	3 检查是否设置口令复杂度	
中间件	HP UX 11i配置模板	4 检查是否设置口令重复使用次数	
网络	Redhat5/CentOS5配置權板	5 检查是否设置口令连续认证失败次数	
安全设备	RedHat6/CentOS6配置價板	6 检查是否设置口令生存周期	
虚拟化/大数据	Redhat7/CentOS7配置模板	7 检查是否删除或锁定无关帐号	
总计7条记录 《 < 1	→ Solaris10配置模板	8 检查是否按用户分配帐号责任到人	
	Solaris11配置模板	9 检查是否禁止root用户远程telnet登陆	
	SUSE 10.X配置横板	10 检查是否关闭系统串行口(serial port)	
	SUSE 11.X配置槽板	11 检查是否按组进行帐号管理	
	SUSE 9.X配置模板	12 检查是否设置用户所需的最小权限	
	Ubuntu配置模板	13 检查是否设置文件与目录缺省访问权限	
	Windows 10配置模板	14 检查是否设置重要文件和文件夹的权限	
	Windows 7/Windows Server 2008配置	15 检查是否禁止不必要的用户登录FTP 置模板	
	Windows Server 2003配置模板	16 检查是否设置控制FTP进程缺省访问权限	
	Windows Server 2012配置模板	17 检查是否禁止匿名FTP	
	Win 8配置横板	18 检查是否启用内核级审核	
	※用6、都再通知	19 检查是否配置日志文件权限	

图 4.6.4 基线模板



五. 脆弱性模板

5.1 基线策略模板

WEBUI: 主界面 -> 脆弱性模板 -> 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 5.1 所示:

🔗 数据安全档	會工具箱系统			0 ③ 2023.12.12 13.49.49 タ 病台電理员 🍝 ④ 原出
	◎資产管理 ◎ 胞弱性检测		○数線探測 ○合規始査 □报告中心 ◎ 系统配置	
二 基础资格相应	日期前性核較/全基建物動模板			
≣ D\$94	▶ 基线策略模板 ▲ 基线离线	戋模板		Î
G WEB#6#	員 基线策略	地加市路 > 〇	▲ 模板类别 全部 * 全部 *	◇ ○ ■検査項 優素合称回年 ◇ ○
③ 系统编件	策略名称	▼ 線作	模板名称	▲ 現則名称
	[工信部]电信网和互联网安全防护	uxun	Oracle 11G for Windows 配置接版	✓已自用 检查是否限制具备数的库超级管理员(SYSDBA)初期的用户远程登录
	[公安部]信息系统安全等级保护基本	5要求	Win 8起置模板	✓已期期 检查口令强能投票
	中国移动管理信息系统安全配置	~~	XenServer 6.x配置换版	✓已向用 检查是否设置数据库用户口令生存用明
	中国电信 (2014) 528号安全配置规	- 28	NETSCREEN防火增配置機板	✓已時期 检查是否追用数据字典保护
	默认安全配置规范	**	IIS7-9配置操板	✓已由用 检查是否设置超过数据库登录失败次数后期定该用户的偏规时间
	总计5条记录	« < 1 > »	DB2 for Unix/Linux配置模板	✓■信用 检查是否设置数据库账户口令到明后常很天数
			Win7/Windows Server 2008配置模板	✓口由用 检查是否禁止用户重复使用规定次数内已使用的口令
			Tomcat 7.x-8.x for Windows配置模板	◆日日用 检查是否设置登录认证方式
			网神与近普(FW3000/4000)系列防火墙配置模板	✓已約期 检查是否设置用户错误口令尝试次数
			Nginx for Linux/Unix西國模板	✓已回用 检查是否打开监听器日志
			Nginx for Windows配置模板	◆已島用 检查是否开启数据库审计日志
			Oracle 12c for Unix/Linux配置機板	✓已启用 检查是否设置数据库监所款(USTENER)启动密码
			Esxi 5.x-6.x配置模板	✓ 民息用 检查是否设置只有信任的IP地址能通过监听器访问数据库
			思科交换机配置模板	✓■協用 检查是否根据机器性能和业务需求,设置最大最小连接数
			TongWeb for windows配置模板	✓已由用 检查是否设置数据库实用性将额时目间
			Redhat/CentOS 6.x配置模板	
			Jboss for Windows 配置模板	Press in an and a second

图 5.1 基线策略模板

5.1.1 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 5.1.1 所示



新增基线策略			×
模板名称 查询条件	* 长度在[4-16]之间 请选择模板类别		
一一己选模板	查询 重置 暂时没有选择筛选条件		
	模板类别	▼ 核查项数量	
	Resin 4.x For Windows配置模板	5	
	Resin 4.x for Linux/Unix配置模板	6	
	Storm配置模板	7	
	WebSphere 7.x for Windows配置模板	8	
	TongWeb for windows配置模板	9	
	Nginx for Windows配置模板	9	
	TongWeb for Linux/Unix配置模板	9	
	Nginx for Linux/Unix配置模板	10	
	Jboss for Windows 配置模板	10	
		10	

图 5.1.1 新建基线策略

5.1.2 基线离线模板

基线离线模板可以提供用户下载,远程对主机进行扫描生成离线结果

离线任务:将在目标靶机上执行的基线核查结果导入到系统,直接进行解析和结果查看, 没有远程登录和检测的过程

🛃 数据安全机	验查工具箱系统		0 © 2023.12.12 13.5027 A 兩台推發於 👻 O 麗田
	O 3029112112 O 3039312140301 O BEGG1216246 M 3538219200		
二 基础实践相反	□ 脂粉性模拟 / ∠ 基础情绪模拟		
5 D\$98	▲ 基线策略模板 ▲ 基线离线模板		
G WEBMAR	■ 横振美別 く ②	山配置機板 ~	○ ▲ 检查项列表
⑦ 系统稿件	模板类别	□ 极振名降	▲ 編号 ⇒ 名称 ▲
	全部	AIX7.1西2面積極於	1 检查是否设置口令失效提示
	主机	Debian 5.x/7.x配置模板	2 检查型否禁用root用户远程ssh
	数据库	Debian 8.x配置模板	3 检查是否设置口令契款度
	中间件	HP UX 11间置操版	4 检查显否设置口令重复使用次数
	网络	Redhat5/CentOS5配置模板	5 检查是否设置口令连续认证失败次数
	安全设备	RedHat6/CentOS6配置模板	6 检查题否设置口令生存周期
	虚拟化大数据	Redhat7/CentOS7配置模板	7 检查是否删除或彻定无关帐号
	总计7家记录 《 〈 1 〉 》	□ Solaris10配置模版	8 检查显否按用户分配账号责任到人
		Solaris11配置機板	9 检查是否禁止root用户远程telnet登陆
		SUSE 10.X政治限制度	10 检查显否关闭系统串行口(serial port)
		□ SUSE 11.X配置模板	11 检查是否按组进行帐号管理
		U SUSE 9.X配置模板	12 检查是否设置用户所需的最小权限
		Ubuntu記證得版	13 检查显否设置文件与目录缺省访问权限
		Windows 10配置模板	14 检查是否设置重要文件和文件夹的权限
		□ Windows 7/Windows Server 2008配置機械	15 检查是否禁止不必要的用户登录FTP
		□ Windows Server 2003配置機械	16 检查是否设置控制TP进程缺省访问权限
		Windows Server 2012配置模板	17 检查是否禁止匿名FTP

图 5.1.2-1 基线模板



离线安全基线检查过程:

(1)选择离线任务后,输入任务名称,选择核查规范

(2)导入离线结果,离线结果支持 xml 或 zip 格式导入,最后选择所需要的告警模板

5.2 口令字典

WEBUI: 主界面 -> 脆弱性模板 -> 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 6.2 所 示:

5		☑ 翻号的性极极	▶ 読品探測		 合規检查 	◎ 报告中心	o real	8								_
线策略模板	C BEALEWAY / 10 C 4494															
令字典	▶ 口令字典														上传字典土	
EB捕件	■ 组合字典			搜索[回车] >		名字典				搜索[回车]	> 0	★ 密码字典			搜索[回车]	1
系统播件	宁典名称	▼ 所属服务	总数	操作	宁典名	称	•	所属服务	总数	操作		宁典名称	▼ 所属服务	总数	操作	
	informix组合字典	informix	181		infor	nix用户名字典		informix	6			informix密码字典	informix	337		
	sybase组合字典	sybase	735		sybas	e用户名字典		sybase	10			sybase密码组合字典	sybase	292		
	https-post组合字典	https-post	1		https	post用户名字典		https-post	1			https-post密码字典	https-post	1		
	http-post组合字典	http-post	1		http-	post用户名字典		http-post	1			http-post密码字典	http-post	1		
	https-head组合字典	https-head	1		https	head用户名字典		https-head	1			https-head密码字典	https-head	1		
	http-head组合字典	http-head	1		http-	nead用户名字典		http-head	1			http-head密码字典	http-head	1		
	https-post-form组合字典	https-post	1		https	-post-form用户名等	字典	https-post	1			https-post-form密码字典	https-post	1		
	https-get-form组合字典	https-get-f	1		https	-get-form用户名字	典	https-get-f	1			https-get-form密码字典	https-get-f	. 1		
	https-get组合字典	https-get	1		https	get用户名字典		https-get	1			https-get密码字典	https-get	1		
	http-post-form组合字典	http-post-f	1		http-	oost-form用户名字	"典	http-post-f	1			http-post-form密码字典	http-post-f	. 1		
	http-get-form组合字典	http-get-f	1		http-	get-form用户名字的	典	http-get-f	1			http-get-form密码字典	http-get-f	1		
	http-get组合字典	http-get	1		http-	get用户名字典		http-get	1			http-get密码字典	http-get	1		
	GlassFish组合字典	GlassFish	1		Glass	Fish用户名字典		GlassFish	1			GlassFish密码字典	GlassFish	1		
	WebSphere组合字典	WebSphere	1		Webs	iphere用户名字典		WebSphere	1			WebSphere密码字典	WebSphere	1		
	JBoss组合字典	JBoss	1		JBoss	用户名字典		JBoss	1			JBoss密码字典	JBoss	1		
	Weblasid@Arth	Wahl onic	1		Mobi	ogic田户名字曲		WebLogic	ī			WebLogic家将字曲	Webl onic	1		

图 5.2 口令字典

5.2.1 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,上传的文件大小正常不超过 10MB。具体如下图 6.2.1-1 所示:



上传字典文件				×
文件内容格式规格 <mark>必读</mark>	文件内容基本要 内容特征要求: 上传格式要求: 文件名称对字符	求: 【 【用户 【只支 限制:	一组换一行、用户名或者密码都不为空、且一组内容长度不超过60】 名:密码 内容特征:用户名和密码用英文':'隔开,且都不为空】 持.dic格式文件。.txt格式文件可以通过修改文件后缀名后上传】 '\''、'`、' '、'\$'、','、'\、''、'\n'、'<'、'>'、'/'、'?'、':'、'''、'('、')'、空格字符	
请选择需要上传的文件 选择文件 未选择任何文 只支持后缀为.dic格式文件	乙件 牛。			
文件内容特征	用户名:密码	٣	请根据上传文件内容选择相对应的内容特征及所属服务类型。	
所属服务	TELNET	٣	注意: REDIS、SNMP服务只能上传密码字典。	
▲上传 ◎重置				

图 5.2.1-1 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 5.2.1-2 所示:

🛛 🔊 数据安全检查:	工具箱系统										२ 前台管理员 ▼	0 ian
=		☑ 龍弱性模板		3現絵曲 回報告中心 令系統語								
∠ 基线策路模板	◎ 胞弱性模板 / 田口令字典											
□ □令字典	▶ 口令字典										上传字典土	Î
G WEBNIN	同 组合字典		捜索[回车] > 2	▲ 用户名字典			捜索[四年] > 2	★ 密码字典			搜索[回车]	~ 0
B 3556394	字典名称	▼ 所属服务	总数 操作	字典名称	所国服务	总数	操作	字典名称	▼ 所属服务	总数	線作	
	informix组合字典	informix	181	informix用户名字典	informix	6		informix密码字典	informix	337		
	sybase组合字典	sybase	735	sybase用户名字典	sybase	10		sybase密码组合字典	sybase	292		
	https-post组合字典	https-post	1	https-post用户名字典	https-post	1		https-post密码字典	https-post	1		
	http-post组合字典	http-post	1	http-post用户名字典	http-post	1		http-post密码字典	http-post	1		
	https-head组合字典	https-head	1	https-head用户名字典	https-head	1		https-head密码字典	https-head	1		
	http-head组合字典	http-head	1	http-head用户名字典	http-head	1		http-head密码字典	http-head	1		
	https-post-form组合字典	https-post	1	https-post-form用户名字典	https-post	1		https-post-form密码字典	https-post	1		
	https-get-form组合字典	https-get-f	1	https-get-form用户名字典	https-get-f	1		https-get-form密码字典	https-get-f	1		
	https-get组合字典	https-get	1	https-get用户名字典	https-get	1		https-get密码字典	https-get	1		
	http-post-form组合字典	http-post-f	1	http-post-form用户名字典	http-post-f	1		http-post-form密码字典	http-post-f	1		
	http-get-form组合字典	http-get-f	1	http-get-form用户名字典	http-get-f	1		http-get-form密码字典	http-get-f	1		
	http-get组合字典	http-get	1	http-get用户名字典	http-get	1		http-get密码字典	http-get	1		
	GlassFish组合字典	GlassFish	1	GlassFish用户名字典	GlassFish	1		GlassFish密码字典	GlassFish	1		
	WebSphere组合字典	WebSphere	1	WebSphere用户名字典	WebSphere	1		WebSphere密码字典	WebSphere	1		
	JBoss组合字典	JBoss	1	JBoss用户名字典	JBoss	1		JBoss密码字典	JBoss	1		
	WebLogic组合字典	WebLogic	1	WebLogic用户名字典	WebLogic	1		WebLogic密码字典	WebLogic	1		
	Tomcat组合字典	Torncat	1	Tomcat用户名字典	Tomcat	1		Tomcat密码字典	Tomcat	1		

图 6.2.1-2 上传口令字典

5.3 WEB 插件

WEBUI: 主界面 -> 脆弱性模板 -> 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 5.3 所示:

羚见数据安全检查工具箱用户手册



🛛 🛃 数据安全检查	工具箱系统					12 135354 A 前白喉環系 • O 副由
2				o sear		
∠ 基线策略模板	⊡ 18891±19.00 / G WEBRAR					
□ 口令字曲	♣ WEB插件					î
G WEBBER	■ 漏洞機板	地加模板 🗸 😋	4. 漏洞美別	~ 0	マ商 マ中 マ低 マ信号	搜索(四年)
 予約編件 	模板名称	▲ 操作	类别名称	总计	жя	
	全部WEB源詞		AI 注入	257	医风险 错误版回注入	
	高/中/低风险WEB漏洞		A2 失效的身份认证和会话管理	21	高限者 aspcms后台cookie 注入	
	高/中风险WEB漏洞		A3 跨站脚本 (XSS)	60	Anwsion people SQL注入漏洞	
	商风险WEB题间	24	A4 不安全的直接对象引用	122	高限台 Anwsion 过滤线将导致SQL注入漏洞	
	总计4条记录	< < 1 > ≫	A5 安全配置错误	73	高风后 Anwsion建始程序注入通到	
			A6 敏感信息泄漏	139	AnyMacro邮件系统登录界面SQL注入漏洞	
			A7 功能极访问控制缺失	109	風风殿 盲注漏洞	
			A8 跨站请求伪造(CSRF)	2	鳳氏版 盲注题词 (数字)	
			A9 使用含有已知漏洞的组件	32	風风殿 窗注题词 (字符)	
			A10 未验证的重定向和转发	5	高风殿 <u>岩注意词 (搜索)</u>	
			总计10条记录	€ € 1 > >	高级趋 盲注篇词 (Cookie内数字)	
					電視台 雷注漏詞(Cookle内字符)	
					高灰岩 盲注漏詞 (Cookie内搜索)	
					等风险 富注漏洞 (字符或-1)	
					高段层 盲注稿詞 (数字或-1)	
					<u>美汉治</u> 恶意抑本	
					· 建风险 盲注通词 (数字或-2)	Ŧ

图 5.3 Web 插件

5.3.1 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 5.3.1-1 所示:

新增漏洞模板					×
模板名称		*长度在[4-16]之间			
查询条件	漏洞名称	请选择漏洞类别	请选择风险	金等级	
	查询 重置				
已选漏洞	暂时没有选择筛选条件				
	漏洞名称			漏洞分类	
	高风脸 齐博CMS V7 job.php	0 任意文件读取漏洞		A7 功能级访问控制制	失
	高风脸 SeaCMS后台命令执行	」漏洞 (CNVD-2020-22721)		A7 功能级访问控制备	失
	高风险 用友NC系统uapws w	vsdI XXE漏洞		A7 功能级访问控制。	失
	高风脸科荣AIO企业管理软件	拉尼程命令执行		A1 注入	
	高风脸 泛微OA E-Weaver Si	gnatureDownLoad 任意文件读取漏洞	l (A6 敏感信息泄漏	
	高风脸 Cacti remote_agent.	php 远程命令执行漏洞		A5 安全配置错误	
	高风险 phpIPAM SQL注入漏	詞 (CVE-2022-23046)		A7 功能级访问控制制	铁
	高风脸 thinkcmf-5.0.190111	I后台任意文件写入漏洞 (CVE-2019-75	80)	A7 功能级访问控制制	柣
	高风脸 EmpireCMS SQL注入	、漏洞(CVE-2022-28585)		A7 功能级访问控制制	失

羚见数据安全检查工具箱用户手册



数据安全检查	工具箱系统					○ 2023-12-12 13-55-02 A 前台管理员 ▼ U 風田
≝.				© 8.66 22		
∠ 基线角器模板	日 服約性規模 / G WEBIAN					
□ 口令字典	♣ WEB插件					î
G WEB554	■ 漏洞模板	第10楼板 > 〇	4. 蒲洞类别	 2 	☑高 ☑中 ☑低 ☑信◎	授素[回车]
医 系统邮件	模板名称	▲ 操作	类别名称	* ⁢	жя	
	全部WEB調調		A1 注入	257	展风般 错误返回注入	
	高/中/低风险WEB激词	-	A2 失效的身份认证和会话管理	21	高风龄 aspcms后台cookie 注入	
	商/中风险WEB週期		A3 跨站脚本 (XSS)	60	高融版 Anwsion people SQL注入通问	
	商风险WEB测测	-	A4 不安全的直接对象引用	122	高风险 Anwsion 过滤器指导致SQL注入漏洞	
	test(admin)	ĭ ×	A5 安全配置错误	73	高良龄 Anwsion建站程序注入运河	
	总计5条记录	κ (1) »	A6 敏感信息泄漏	139	和INMacro邮件系统登录界面SQL注入漏洞	
			A7 功能级访问控制提供	109	風风脸 盲注漏洞	
			A8 跨站请求伪造(CSRF)	2	<u>無风险</u> 盲注配词 (数字)	
			A9 使用含有已加温润的组件	32	哀风悠 盲注職詞 (字符)	
			A10 未验证的重定向和转发	5	高风险 盲注職詞 (搜索)	
			总计10条记录	« (1) »	高风险 盲注漏洞(Cookie内数字)	
					高风始 盲注漏洞(Cookie内字符)	
					高风险 盲注漏洞 (Cookie内搜索)	
					温风龄 盲注漏洞(字符或-1)	
					高风龄 盲注漏洞(数字或-1)	
					展风险 思意脚本	(1) 提示 添加服用等例复成功
					展风险 盲注漏洞(数字或-2)	v

图 5.3.1-1 新增 Web 插件模板

5.4 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 6.4 所示:

8	○ 第产数量 ○ 数形性检测	回 脱裂性结核 一座 肥料	1973年 〇 1995年2月 〇 合現絵曲 〇 安告中心	© XKAN	
基线策略模板					
口令字典	▶ 系统插件				
WEB描件	■ 漏洞模板	AND	○ 山漏洞美別 潮洞美別 *	ŝ	C 図商 ☑中 ☑低 ☑信息 ● 控索名称/强号/CVE/CNNVD/年俗/系统
系统新件	模板名称	▲ 操作	类别名称	▲ 总计	漏洞
	全部建制扫描		SQUEA	13328	Symantec Web Gateway远程命令行管理程序命令执行漏洞
	原理識词扫描	122	Web应用	3354	Symantec Web Gateway远程命令行管理程序命令执行题词
	Linux通用描	1075	安全特征	1522	医Que Symantec Web Gateway多个流河
	Windows激励扫描	1.000	边界条件错误	1485	WordPress Backupbuddy多个漏洞【图理扫描】
	MacOS識詞扫描	355	代码问题	12155	Wordpress WP Mobile Edition 插件远程文件建器漏洞
	数据库藏词扫描		代码主入	7054	WordPress Multi View Event Calendar存在SQU注入漏洞
	数据库安全漏洞[数据库]	32	访问控制	19499	WordPress UserPro 插件认证探过漏洞
	高/中风险系统融词		格式化学符串	1083	Wordpress Zip Attachments 插件 "download.php" 目录遍历调制
	高风险系统漏洞	140	国产数据库	66	WordPress Portable phpMyAdmin 'wp-pma-mod'安全编述漏洞
	历年攻防热门藏词	22	国产应用	91	IIII WordPress Photoracer 插件'id'参数SQL注入週间
	总计10条记录	< < 1 >	「言語接	2013	- WordPress-MU wp-login.php 安全绕过漏洞
			环境条件	565	WordPress MailPoet插件文件上传稿词【原理扫描】
			德中区溢出	58589	WordPress WPI论坛服务器"topic"参数SQU主入漏洞
			10221000	4919	WordPress Nmedia成员对活播的任意成文件上传输制度
			竞争条件	3416	Nordpress IBS Mappro目录遍历能洞【傅理组指指】
			拒绝服务	14	BRM WordPress BackWPup 插件'wpabs'参数远程PHP代码执行题词
			跨站脚本	30796	Wordpress Work Flowl语件 文件上传遍洞

图 5.4 系统插件

5.4.1 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 5.4.1-1 所示:

新增漏洞模板					×
模板名称		* 长度在[4-16]之间 [提示: 切换漏	洞等级时,所自定义模板的漏洞等级可能	徐变更,但不影响检测任	务]
模板类别	● 系统模板 ○ 数据库模板				
查询条件	漏洞名称	CVE-或CNCVE-或CNVD-或CNN	请选择漏洞级别	▼ 至	
					*
	请选译操作系类别	请选择应用类别	请选择服务类别		
					-
	查询 重置				
已选漏洞	漏洞名称		▲ 漏洞分类		
	没有检索到数据				
	总计0条记录			« < >	»
	保存				

8	○ 約22世間 ○ 動動性松湖		RM ② 1655月2月 ② 合現絵曲 □ 165年0	© 20022	
基线策略模板	□ 施弱性疾病 / □ 系统编件				
口令字典	▲ 系统插件				
WEBMM4	周 瀧河模板	端加模板	○ ▲ 漏洞类別 *		 ○ 図高 図中 図低 図信息 ● 授売名称/論号/CVE/CNNVD/年份/系統
系统漏件	极板名称	▲ 展作	类别名称	≜ abit	3634
	全部漏洞扫描	1.44	SQLEA	13328	高风险 Symantec Web Gateway远程命令行管理程序命令执行漏洞
	原理漏洞扫描	12	Web应用	3354	aggab Symantec Web Gateway远程命令行管理程序命令执行赢同
	Linux調測扫描	100	安全特征	1522	axxxb Symantec Web Gateway多个識問
	Windows調調扫描		边界条件错误	1485	addada WordPress Backupbuddy多个潮洞【原理扫描】
	MacOS篇词目描	1.55	代码问题	12155	NDAM Wordpress WP Mobile Edition 插件远程文件泄露漏洞
	数据库赢洞扫描		代码注入	7054	wordPress Multi View Event Calendar存在SQU主入通用
	数据库安全漏洞[数据库]	100	访问控制	19499	asalas WordPress UserPro 播件认证规过编码
	高/中风险系统赢词	575	格式化字符串	1083	Wordpress Zip Attachments 插件 "download.php" 目示追历論詞
	高风险系统演问	0.000	国产数据库	66	WordPress Portable phpMyAdmin 'wp-pma-mod'安全统过漏洞
	历年攻防热门漏洞	-	國产应用	91	高校 MordPress Photoracer 插件'は'参数SQLi主入通问
	test(admin)	(2° ×	后置链接	2013	NordPress-MU wp-login.php 安全统过编词
	总计11条记录	K (1)	环境条件	565	NULL WordPress MailPoet插件文件上传版词【原理扫描】
			缓冲区溢出	58589	WordPress WP论坛服务器"topic"参数SQL注入漏洞
			加坡的问题	4919	WordPress Nmedia成员对话插件任意文件上传篇词
			荒争条件	3416	Wordpress IBS Mappro目录遍历湖湖【原理扫描】
			拒绝服务	14	展现版 WordPress BackWPup 插件'wpabs'参数远程PHP代产物中态词
			時站脚本	30796	展现数 Wordpress Work Row插件 文件上传遍消

图 5.4.1-1 新增系统插件模板

① 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。


六. 流量探测

WEBUI: 主界面 -> 流量探测

流量探测包括新建任务、探测预览页面,其中探测预览中包括10种不安全行为预览。

6.1 新建任务

WEBUI: 主界面 -> 流量探测 ->新建任务

6.1.1 新建任务

流量探测页面可以根据 IP 段、探测类型、探测时间段、API 存活探测新建不同的任务, 其中探测类型预计支持 API 与数据库两种,目前只支持 API 类型, API 类型中只支持 http 类型的流量探测。探测时间段可分别选中 5 分钟/10 分钟/1 小时/2 小时, API 存活探测,选是时会进行 API 存活的探测,并在 API 清单列表中新增相应的记录,选否不进行 API 存活探测。

≷ 数据安全检查:	L具箱系统														
	0 871111	0.00000000		ler 12/2019/201	0 6087788	⊙ nRita	■18890	© \$6667							
© NIDES	la 10.80928 / 🖸	的政任的													
D. 深刻積終		5													
	•任务名称	GREE						- BR380-152	太孙治会使用 示:	Re172310.1.172310.3-1	172,310,255			 # #	
	• IF20000	AFI					~	· IFINIPALIANO	W0.077810-F00				v		
	API存法原则	8					v								
	109.85														
	iBiji D	法成													
	1817		488 8	(ERM	1000141	(18s	crititati-i		5438001647	19936912		STREET.	APIFERSEN	WHERE	18m
										60 167,253					

图 6.1.1 新建任务

6.2 探测预览

WEBUI: 主界面 -> 流量探测 ->探测预览

6.2.1 探测预览

探测预览页面展示探测完成任务的安全情况,及所有探测任务的综合概况。安全总览展 示探测次数,以及探测结果中安全与不安全事件总数。右侧不安全行为预览即17种不安全模 型对应的事件,若触发对应事件即说明流量片段非安全。

当前模型包括: cookie 中包含密码、数据泄露风险、敏感数据导出、单次返回数据量过



大、敏感数据传输、api参数可遍历、明文传输密码、机器访问行为、命令执行 api、访问超限、明文传输弱口令、数据库查询 api、未鉴权访问、数据出境风险、出境账实不符、持续数据泄露、账号高频访问。

任务详情展示所有已完成的探测任务,及相关参数与安全与否。不安全的任务将展示具体安全行为内容,点击"详情"即可查看。

探测预览数据保留 30 天数据。

🔊 数据安全检查	工具箱系统											众│⊙2024.07.0	8 16:36:42	○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○	员 ▼ │ ① 退出	
ē	◎ 资产管理		☑ 脆弱性模板	は 流量探測	⊙ takasisiking	⊙ 合规检查	☑ 报告中心	© 系統配置								
新建任务	區 流量探測 / 日	3 探测告警														
· 探測告答	告警总览				6	不安全行为预览										
		深刻任ちら数 4个	 API: 安全 不安 	4087800次 274476次 全: 3813324次		3,000,000 2,500,000 1,500,000 1,000,000 500,000 0 0 0 0	1 7 88.878.5788 908.978.5788 90.588	16 3 2734 4 55年間間1月2日 55日間1月2日 55日間1月2日 55日間1月2日 55日 55日 55日 55日 55日 55日 55日 55日 55日 5	373382 1324162 1424162 1545 1511	2014323 196381 196381 01 ⁷⁷ 8 4 96 ⁷	118 9 是 成婚姻的 ^{公会} 教授成章	2790768 624227	0 0 80 100 10 10 10 10 10 10 10 10 10 10 10 10	0 0 References		
	探测类型	全部		v	探測量	10 #20610			✓ 任务	洛称 任务名称			*	展开 Q 1	前 C 重重	
	客户端IP	客户端IP 示例:1	72.31.1.1		服务	NP 服务IP 示例	172.31.1.1		接口	11地址 接口地址 万	例: http://ww	w.a.com/api				
	任务详情															
	序号	任务名	探测类型	采测时间 客	⊐端IP	服务IP	服务端口	接口地址	传输包大小	任务创建时间	是否安全	不安全行为	命中起数	API存活数	操作	
	1	ALL-TEST	API	17	2.20.54.18	172.20.54.23	19980		25 B	2024-07-07 19:	是		15088	16	详情 删除	
	2	ALL-TEST	API	17	2.20.54.19	172.20.54.23	19980	http://172.20.5	1.24 kB	2024-07-07 19:	否	机器访问行为	162595	16	详情 删除	
	3	ALL-TEST	API	17	2.20.54.18	172.20.54.23	19980	http://172.20.5	1.76 kB	2024-07-07 19:	否	未鉴权访问	60283	16	详情 删除	
	4	ALL-TEST	API	17	2.20.54.53	172.20.54.23	19980	http://172.20.5	1.24 kB	2024-07-07 19:	否	未鉴权访问	65668	16	详情 删除	

图 6.2.1 探测预览



七. 敏感探测

7.1 数据库资产

WEBUI: 主界面 -> 敏感探测 -> 数据库资产

对数据库进行深度扫描,100+敏感字段规则风险发现数据库中的敏感字段。

			0.9838 0.98380 0.9839-0	() () minimum					
数据有关产	○·他很印刷 / ₩ 數攝業表产								
机感致需发现	资产名称 而产ET			BERRY DETAIL			PBH DISTRICT		4.89 C 22
	#Q	资产名称	20894208	数把件关型	PROL	東岸医道	Faith	法律状态	86
	4	172.20.51.118	0		172.20.51.118	2 ^m /ž	12		iria musivus
	2	172.20.51.132	0	-	172.20.51.132	医甲基	100 100	177.	irit misiva
	3	172.20.51.136	0	-	172.20.51.136	\$72			注题 机磁环器
	4	172.30.51.137	0	-	172.20.51.137	3°E			irig masava
	5	172.20.51.154	0		172.20.51.154	875			an and an and a second second
	.4	172.20.51.173	1	mysol	172.20.51.173	3°E	11	0个感到1个失败	は提 解释法理
	7	172.20.51.65	0		172-20.51.65	±*Z			(FIG 40.06(F30
	8	172.20.54.245	0		172.20.54.245				irig misirin
	9	0001	0	1.72	172-20.57.12	285			计语 机加尔加
	10	DC-BOX/RBIT/TL	4	Hive数据库,mariado,MongoD的数据库,mysql	172.20.57.51	SHE		計成这1个关放	计值 机运行机
									< 1 2 ×

图 7.1 数据库资产

7.1.1 数据库列表

WEBUI: 主界面 -> 敏感探测 -> 数据库资产-> 数据库列表

资产管理中的所有数据库资产会在表单中显示。

- 2	OSTER ORRECT	CARDER LEASE ON	CARLE CREPO	日本時間間					
1438/*	CONSIGNATION AND ADDRESS OF								
感激频发现	8#88 8**58			NRAZO DECAD		×	PHM DEFENS		Q MR C II
	2524718 (VAL22								
	库号	展产名件	BRARS	数据库类型	IP INTE	医产泡油	新聞秋念	9842	100
	1	172.20.51.118	0	24	172.20.51.118	3**2	122.0	1.000	urit Antescon
	2	172.20.51.132	ø	-	172.20.51.132	2 ⁴⁶ £		-	1210 ANSIVA
	3	172.20.51.136	0		172.20.51.136	±#8			11110 M1855730
	4	172.20.31.137	0		172.20.51.137	2*2			1215 40151936
	5	172.20.51/154	0		172.20.51.154	##3			1215) 40.5519.30
	4	172.20.51.173		mysel	172.20.51.173	3#E		01個別11個限	1215 40.151930
	7	172.20.51.65	0	144	172.20.51.65	生 単区	344	120	urth stassym
	8	172.20.54.245	0		172.20.54.245				ivia atustivat
	4	0001	0	177	172.20.57.12	100	5 115 5		trig ensives
	10	DC-BOXINGH.	4	Hive数据库,markado,MongoDR数据库,mysql	172.20.57.51	±=S		计成批计关数	FFIS MISIFIN
									< 1 2 2

图 7.1.1-1 数据库列表

点击详情可以配置数据库的详细信息,点击'点击连接'可以测试是否能正常连接。如 果连接成功,下方的统计会显示数据库的详细信息。



助上: 172.20.51.118	资产名	呂称: 172.20.51.118	数据库数量	赴: 0		数据	库类型:	
≃区域: 生产区								
) 当数据库类型是 oracle 时,填写,	用户名时,需带上角色 例子	: user as 角色名						
数据库配置								添加
牧据库名称	数据库类型	数据库端口	用户名		密码		操作	
请输入数据库名称		∧ 请输入数据库端口	请输入用户名		请填写密码	ø	点击连接	
	mysql							
	mariadb							
统计	oracle							
应导 数据库 实称	sqlserver	空码数	志勤招导	空段洋塘				
AP 3 SOME LITY	postgresql	7 - 200	ACIANITE	- 7 - 2				
	greenplum							
	些为高斯100		U					
	19914/01/00		暂无数据					

图 7.1.1-2 添加数据库资产

参数	说明
数据库名称	显示当前任务的名称
数据库类型	选择的类型有 mysql、mariadb、oracle、sqlserver、postgresql、greenplum、达梦 数据库、华为高斯 100、TIDB、巨杉数据库、Hive 数据库、MongoDB 数据库
数据库端口	根据不用的数据库类型来输入相应的端口
用户名	输入数据库的用户名
密码	输入数据库的密码

如果有连接成功的数据库,此时点击敏感探测就可以对数据库进行敏感数据扫描。

			731 〇 A 昭和臣 - 回 昭和中心	DEMAIN					
明年後产	OVER / H DEVET								
的意思的发展	8/*20 5/~50			BWCHT DECET		v.	164 1:5512		9, 200 C 20
	の現立2月8 好政治支								
	R.G.	8/18/0	25/8/W25/92	2.8422	or Hald	RP/RM	Ratio	法接受力	10rs
	1	172.20.51.118	0		172.20.51.118	生产区		-	eritä e ksisteran
	2	172.20.51.132	0		172.20.51.132	生产区			计插 机感探测
	1	172.20.51.136	0	<u></u>	172.20.51.136	±*2	100	14	1715 ML06193H
	4	172.20.51.137	0	77	172.20.51.137	生产区	15	77	1210 BLISTON
	*: *:	172,20,51,154	0		172.20.51.154	±772	100	-	1715 M1061F30
	6	172.20,51.173	1	mynal	172.20.51.173	生产区		0个成批1个大效	iria misirm
	7	172.20.51.65	D		172.20.51.65	生产区	22	2	iria morra
	8	172.20.54.245	0	**	172.20.54.245				1715 MIMIFUN
	9.)	0001	0		172.20.57.12		144		计输 敏感探测
	10	DC-BCKREZM	4	Hive認識者 mariado MongoDB認識者 mysql	172.20.57.51	±rE		计成功1个关键	1718 MI161930
									× 1 2 >

图 7.1.1-3 敏感探测

7.1.2 探测进度

WEBUI: 主界面 -> 敏感探测 -> 数据库资产-> 探测进度

点击了敏感探测的数据库会在这里显示进度。点击"开始",重新进行敏感探测。探测中的资产,点击"终止",暂停对应的敏感探测。

B O #rrbit O Excellati O Excellati O #likitivity O #likititity O #likitivity <t< th=""><th></th><th></th><th></th><th></th><th></th><th></th><th>-</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></t<>							-											
NAME NOTIFIE N		æ	0 8/127		N 🖸 KARANARAN	la serien	© MRMINI	○台開始音	□報告中心	O RIGHT								
NAME NAME <th< th=""><td></td><td>数据库资产</td><td>C constant / w</td><td>和341年日/**</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></th<>		数据库资产	C constant / w	和341年日/**														
NUME-P1 RPACH REAL PEAL REAL	INTER INTER <th< td=""><td>國政策发現</td><td>资产名称</td><td>8788</td><td></td><td></td><td></td><td></td><td>数据库关型</td><td>医本关型</td><td></td><td></td><td>UP IP IP</td><td>te anna anna</td><td></td><td></td><td>く重日</td><td>С</td></th<>	國政策发現	资产名称	8788					数据库关型	医本关型			UP IP	te anna anna			く重日	С
A-9 RF-FA RESERVED IPENL <	№9 №7-68 №86.927 №91.00 №70.000 №20.0		数据库列表	PRER														
1 2004-04-30 154-106 449 6,43 5 710 R1911			库号		资产名称	截寇库美型	IP	地址	1至300年18		採測表数	探测状态	量近探发时间	FINED	敏感表量/总表量	探测次数	操作	
BUTR < 🚺 >			1		基线検査-172.20.57.28	myaql	17	2.20.57.28	2		53	已完成	2024-04-30 15:41:06	410	6/53	5	开始	
																共计1条	< 1 >	10 余/

图 7.1.2 探测进度

7.2 敏感数据发现

WEBUI: 主界面 -> 敏感探测 -> 敏感数据发现

已经敏感探测完的数据会在这里进行展示。数据库检索可以选择想要展示的数据库。

🕐 数据安全检	查工具箱系统						0 © 2004.01.00 m/s0.42 A 1	nomen - (omo)
a		DESCRIPTION OF STREET		1				
H BHCSP	O WARDE / + WEEKEE							
- WERRER	BR8438 1723032135/10	5 + test V						
	福祉会議院 創設的中記時: test IP時代社: 172,20,32,135		和学名称: 1722052135 (中午15歳)	REDWORD: TOO	BYER BALL: 4700			
	非收缩器	0 ####	0 (1997) (1997)	日月前の学校 🚾 転営学校			Pastine -	0108 0
	6860 BEL4557	0 ###7650	0 98747632	6974	@4050	7608 - 49808 C		9. 放麻 C 重要
	#2712							1. 2017-W
	89	****	8日間	敏感中國/总平爾	MNYG	6413	18rs	
				() 47.50/8				

下方的敏感表导出可以导出具体的敏感字段。

图 7.2-1 敏感数据发现结果



也可以通过检索后来导出所要查询的敏感表,导出的内容是检索后的全部库表,具体方法:输入检索条件后,点击查询,库表列表显示信息后,点击离线下载,最后输入任务名称, 点击创建任务即可。

表名称: 01-09		敏感字段:		命中时间:			
E务名称 请指	输入待创建任务的名称	创建任务					
风险资产列	表						
序号	任务名	库表数量	进度	开始时间	耗时	操作	[
1	NICE	409		2024-01-26 10:13:34	22.00 秒	下载删除	
2	bbbb	59		2024-01-25 16:48:15	907.00 秒	下载 删除	
3	eeee	46		2024-01-25 16:47:19	15.00秒	下载 删除	
4	32323	0		2024-01-25 16:46:20	0.00 秒	下载 删除	
5	999999	59		2024-01-25 15:19:47	217.00 秒	下载 删除	
6	asdasdad	0		2024-01-25 15:16:31	0.00 秒	下载 删除	
7	333333	0		2024-01-25 15:10:57	0.00 秒	下载 删除	
8	3333	0		2024-01-25 15:09:35	0.00 秒	下载 删除	
9	aaaa	0		2024-01-25 15:08:38	0.00 秒	下载 删除	
10	DCbox数据库_边界指纹			2024-01-22 16:48:24	4.00 秒	下载 删除	
						共计10条 〈 1 〉 10	条/页∨

图 7.2-2 离线下载



八. 合规检查

8.1 法规合规检查

WEBUI: 主界面 -> 合规检查 -> 法规合规检查

进入法规合规检查页面,可以查看当前支持检查的法规列表

数据安全检查]	[具箱系统				û © 2023.	09.28 13:31:44	A dcbox 👻 ①退出
E	◎ 资产管理	◎ 脆弱性检测 回 脆弱性模板 ■	』 流量探測 ○ 敏感	「「「「」」」 「「」」 「「」」 「「」」 「「」」 「「」」 「「」」			
② 法规合规检查	⊙ 合規检查 / ○ 法規	观合规检查					
目 知识库	道 9	不合规项 检测项总数 9	③ 法规知识周	核验 前往 知识库 ,查看对应条目			
	法规标准分类	着前令法规标准 v 对应法规标准	佳细则 请输入对应法规	合规状态 请输入合规状态 v			Q 査狗 C 重置
	法规列表						
	序号	检查项分类	法规标准条目	对应法规标准细则	合规状态	检查进度	操作
	1	中华人民共和国数据安全法	第二十三条	国家建立数据安全应急处置机制。发生数据安全事件,有关	不合规	已完成	取证原文 复测
	2	中华人民共和国数据安全法	第二十五条	国家对与维护国家安全和利益、履行国际义务相关的属于管	不合规	已完成	取证原文 复测
	3	中华人民共和国数据安全法	第二十九条	开展数据处理活动应当加强风险监测,发现数据安全缺陷、	不合规	已完成	取证原文 复测
	4	中华人民共和国数据安全法	第三十条	重要数据的处理者应当按照规定对其数据处理活动定期开展	不合规	已完成	取证原文 复测
	5	中华人民共和国数据安全法	第三十一条	关键信息基础设施的运营者在中华人民共和国境内运营中收	不合规	已完成	取证原文 复测

图 8.1-1 法律法规检查

点击"取证原文",可以查看流量探测中命中相应法规的任务详情信息,点击"复测" 按钮,会重新启动相关的流量探测任务。

🔊 数据安全检查工			
三 注报会报检查		×	
目知识库	法规编要 国家建立教授之今伯龟所署和制,将生教授之今事件,有关主禁惩门的头统注户动府龟砾要,坚即归的的府龟所署提施,防止各人	書扩十	取证原文 复测
	商家施工政施文主体地交上局が時、交工政施支工学行、ドウ人工自由「J加コドルロキルL®DOK」、本体旧加口J加め上員目前。のJLMで 簡恵、并及时向社会发布与公众有关的警示信息。	53 //, HM/XI	取证原文 复测
		全部收起	取证原文 夏澜 取证原文 复测
	#1 任务名称 Nice-Test-07 客户端P 172205058 服务端P 1722057.101 不安全行为 敏感数据传输	▲ 收起详情	取证原文 复测
	request: [GET/zentao/bug-browse-36-0-unclosed-0-id_desc.html HTTP/1.1 Host: 172.20.57.101		取证原文 复测 取证原文 复测
	Connection: keep-alive Upgade-Insecure:Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36		取证原文 复测
	Accept: tex/tmin.application/xhtmi xml.application/xmlq=Us.mage/avti.mage/apng:7*,q=0.8,application/signed=exchangev=b.sq=0.7 Referen: thttp://172.05.710/jzentas/bug-create=36-0-moduleID=0.html Accept-Encoding: gzip_deflate		取证原文 复测
		确定	

图 8.1-2 取证原文

8.2 知识库

WEBUI: 主界面 -> 合规检查 -> 知识库



进入知识库页面,可查看具体的法规列表及详情信息,列表可根据法规标准分类、法规标准细则分类进行检索查询。

📀 数据安全格	金查工具箱系统				Q │	13:32:00 A dcbox 🔻 ① 退出
	◎资产管理	◎ 脆弱性检测 ◎ 脆弱性模板	□ 流量探测 ② 敏振	蔡探測 ○ 合規检查 □ 报告中心 □ 系統配置		
② 法规合规检查	○ 合规检查 / 目知は	只库				
目 知识库	法规标准分类	请输入法规标准分类 > 法规标准线	田则 请输入法规标准细则	W		Q 直询 C 重置
	法规列表					
	序号	法规标准分类	法规标准条目	法规标准细则	操作	
	1	中华人民共和国数据安全法	第一条	为了规范数据处理活动,保障数据安全,促进数据开发利用,	详情	
	2	中华人民共和国数据安全法	第二条	在中华人民共和国境内开展数据处理活动及其安全监管,适用] 详情	
	3	中华人民共和国数据安全法	第三条	本法所称数据,是指任何以电子或者其他方式对信息的记录。	详情	
	4	中华人民共和国数据安全法	第四条	维护数据安全,应当坚持总体国家安全观,建立健全数据安全	È 详情	
	5	中华人民共和国数据安全法	第五条	中央国家安全领导机构负责国家数据安全工作的决策和议事协	» 详情	
	6	中华人民共和国数据安全法	第六条	各地区、各部门对本地区、本部门工作中收集和产生的数据及	2 详情	
	7	中华人民共和国数据安全法	第七条	国家保护个人、组织与数据有关的权益,鼓励数据依法合理有	ī 详情	
	8	中华人民共和国数据安全法	第八条	开展数据处理活动,应当遵守法律、法规,尊重社会公德和伦	3 详情	
	9	由他人民共和国物理完全注	協力包	国家支持工展新提会个印记宣传基环 追宣令计个的新提会令	、 洋佳	

图 8.2 知识库



九. 报告中心

9.1 资产报告导出

WEBUI: 主界面 -> 报告中心 -> 资产报告导出

资产报告导出可导出资产台账全览、流量报告导出、综合报告导出内容,导出完成后, 下方历史导出记录同步新增一条导出记录。

点击"报告下载",可下载已有记录的报告。

🔗 数据安全检查	王具箱系统				□ ○ 2024.05.07 20:01:47 A 前台管理员 ▼ U 銀出
			o o simul		
ビ 麦产服装导出	□ 報告中心 / ピ 資产報告専由				
12 脱钙性导生	 ● 新建导出任务 ● 服告各件 ● 服告件件 ● 服告件支 ● 服告件支 ● 服告件支 ● 服告件支 ○ 服告 ○ 照告 ○ 照告	5790 I I			
	历史导出记录				
	成号	任务名称	报告种类	服告导出的问	操作
	1	sest1	说 ²⁴ 台标全吃流量报告。综合报告	2024-04-30 19:38:39	腳輪 报告下载
	2	testiadiad	综合报告	2024-04-30 00:45:37	副軸 报告下载
	3	综合导出	综合报告	2024-04-30 00:42:04	删除 报告下载
	4	text@ft	综合报告	2024-04-30 00:15-40	副論 报告下载
	5	90	1961RT	2024-04-30 00:06:46	副號 现而下现
	6	流量报告	流量报告	2024-04-29 15:54:09	删除 报告下载
	7	综合报告等出	综合规则	2024-04-29 15:42:47	副糖 现于下取
	8	test_pmi资产合领	治/**白标全流	2024-04-29 15:29:11	副職 短四下號
	9	嘉纯 续查-172.20.57.28	资产后账金凭	2024-04-29 15:26:12	腳鏡 报告下助
	10	test4512-MB	资产台联全流说量项告综合报告	2024-04-29 15:11:37	副除 短舌下颌
					共計12級 < 1 2 > 10 条/页√

图 9.1 资产报告导出

9.2 脆弱性导出

WEBUI: 主界面 -> 报告中心 ->脆弱性导出

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。

9.2.1 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

▲ 导出报表 ◎ 报表列表 ▲	▶ 报表模板		
输出报表			
选择导出模式	 接任务 按资产 		
任务名称	请选择任务		*提示:请选择需要导出的任务 (支持多选,不支持存活任务)
导出格式	🖲 HTML 😈 🔿 WORD 👿 🔿 PDF 🔎	O EXCEL 🗙 O XML 📶	* 提示:包含基线任务时,不可导出PDF格式
导出方式	详细报表	*提示:请选择导出方式。基线任务仅支持统计报表导出	
导出文件名		*提示: 请填写导出的文件名称。限制: [1-42]字符之间,限制	字符: /**<> ()`{}&;\$:?
设置压缩包密码	×		
是否展示弱口令密码	1		
报表模板	默认模板 ▼	* 提示: 请选择报表模板	
导出			

图 9.2.1-1 导出报表

2)选择配置导出的报表参数,如下

表 9.2.1-1 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
任务历史执行时间	开启可选择该任务某次扫描的结果
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

1) 点击导出,跳转到报表列表界面,展示导出的进度



羚见数据安全检查工具箱用户手册

▲ 导	出报表 12 报表列表 14 报	表模板				刷新€ 搜索回到	车]
	报表名称	报表类型	报表档式	所属用户	导出进度	生成日期	▼ 操作
	[172.20.57.43]_pdf_基线核查-172.	统计报表[任务外发]	PDF	admin	所选目标无扫描任务或者无资产数据	2023-05-06 17:48:02	下载 删除
	[172.20.57.43]_pdf_172.20.50.203	统计报表[任务外发]	PDF	admin		2023-05-06 17:25:05	下载删除
	[172.20.57.43]_pdf_172.20.57.42核	统计报表[任务外发]	PDF	admin		2023-05-06 17:02:06	下载删除
	172.20.57.42标准扫描.zip	详细报表	PDF	admin		2023-05-06 16:54:36	下戴删除
	三方漏扫报告.zip	详细报表	HTML	admin		2023-05-06 16:42:53	下载 删除
	172.20.57.42标准扫描.zip	详细报表	PDF	admin		2023-05-06 16:41:02	下载 删除
	172.20.57.42标准扫描.zip	详细报表	PDF	admin		2023-05-06 16:39:23	下载 删除
	[172.20.57.43]_pdf_172.20.52.230	统计报表[任务外发]	PDF	admin		2023-05-06 16:12:15	下载删除
	[172.20.57.43]_pdf_172.20.54.202	统计报表[任务外发]	PDF	admin		2023-05-06 16:12:05	下載 删除
	[172.20.57.43]_pdf_数据库检测-17	统计报表[任务外发]	PDF	admin		2023-05-06 15:51:04	下载 删除
	[172.20.57.43]_pdf_172.20.57.42核	统计报表[任务外发]	PDF	admin		2023-05-06 15:46:04	下载 删除
	[172.20.57.43]_pdf_172.20.57.42核	统计报表[任务外发]	PDF	admin		2023-05-06 15:31:04	下戴 删除
	[172.20.57.43]_pdf_数据库检测-17	统计报表[任务外发]	PDF	admin		2023-05-06 13:42:03	下载删除

图 9.2.1-2 导出报表

~	·导出报表 · 记 报表列表 ·	▶ 报表模板				刷新ご 投索	回车]
	报表名称	报表类型	报表格式	所属用户	导出进度	生成日期	▼ 操作
	[172.20.57.43]_pdf_基线核查-	-172. 统计报表[任务外发]	PDF	admin	所选目标无扫描任务或者无资产数据	2023-05-06 17:48:02	下载 舱
	[172.20.57.43]_pdf_172.20.50	0.203 统计报表[任务外发]	PDF	admin		2023-05-06 17:25:05	下载 删
	[172.20.57.43]_pdf_172.20.57	7.42% 统计报表[任务外发]	PDF	admin		2023-05-06 17:02:06	下载制
	172.20.57.42标准扫描.zip	详细报表	PDF	admin		2023-05-06 16:54:36	下载 删
	三方漏扫报告.zip	详细报表	HTML	admin		2023-05-06 16:42:53	下载 删
	172.20.57.42标准扫描.zip	详细报表	PDF	admin		2023-05-06 16:41:02	下载 删
	172.20.57.42标准扫描.zip	详细报表	PDF	admin		2023-05-06 16:39:23	下载 册
	[172.20.57.43]_pdf_172.20.52	2.230 统计报表[任务外发]	PDF	admin		2023-05-06 16:12:15	下载量
	[172.20.57.43]_pdf_172.20.54	4.202 统计报表[任务外发]	PDF	admin		2023-05-06 16:12:05	下载量
	[172.20.57.43]_pdf_数据库检测	则-17 统计报表[任务外发]	PDF	admin		2023-05-06 15:51:04	下载量
	[172.20.57.43]_pdf_172.20.57	7.42% 统计报表[任务外发]	PDF	admin		2023-05-06 15:46:04	下载册
	[172.20.57.43]_pdf_172.20.57	7.42% 统计报表[任务外发]	PDF	admin		2023-05-06 15:31:04	下载册
	[172.20.57.43]_pdf_数据库检测	则-17 统计报表[任务外发]	PDF	admin		2023-05-06 13:42:03	下载量
	[172.20.57.43]_pdf_172.20.57	7.42》 统计报表[任务外发]	PDF	admin		2023-05-06 11:49:06	下载 册
	[172.20.57.43]_pdf_已有靶机	扫描_ 统计报表[任务外发]	PDF	admin		2023-05-06 03:39:11	下载量
	[172.20.57.43]_pdf_已有靶机	扫描_ 统计报表[任务外发]	PDF	admin	所选目标无扫描任务或者无资产数据	2023-05-05 15:03:03	下载 删
	[172.20.57.43]_pdf_172.20.57	7.42% 统计报表[任务外发]	PDF	admin			下载册
	[172.20.57.43]_pdf_172.20.57	7.423 统计报表[任务外发]	PDF	admin		2023 ① 提示 下载报表成功	
	[172.20.57.43]_pdf_172.20.57	7.423 统计报表[任务外发]	PDF	admin		2023-05-05 11:18:03	下載 册

2) 报表导出成功后可在报表列表点击下载

图 9.2.1-3 导出报表完成

9.2.2 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 10.2.2-1 所示





图 9.2.2-1 报表列表

9.2.3 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

9.2.3.1 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:



1 检测	结果综述				目录
本) 松 	☆松測中, 扫描 到漏洞共139 到腸口令共0- 风险等级为♥	1 检测结果综还 2 任务总体概览 2.1 任务基本信息 2.2 敏感由问报务 2.3 敏感中问供			
2 任务	总体概览				2.3 或医中间中 3 资产信息统计
2.1 任	月基本信息				3.1 第二/服务统计 3.2 资产风险等级
任务名	称	172.20.50.203			3.2.1 主机资产风险 3.2.2 WEB资产风险
扫描目	标	172.20.50.203			4 漏洞信息统计
北京橋	i#6	野江梅梅			4.1 受影响资产统计
任务部	在账号	admin			4.1.1 系统漏洞影响资产
扫描版	ha	至統扫描・2023-05-06 15:43:18 至 2023-05-06 16:01:14 / 軒时・12	(\ \\$6≸\)		4.1.2 WEB漏洞影响资产 4.2 漫调等级公布
J-JJHH		Web扫描: 2023-05-06 16:01:21 至 2023-05-06 17:24:29 (鲜时 · 1	小时23分)		4.3 漏洞类别统计
		□会積軽: 2023-05-06 16:01:21 至 2023-05-06 16:30:55 (鮮时 · 29	☆34秒)		4.3.1 系统漏洞美别
系统器	本	V3.0(6.6.1-R1-v90757-20230222)			4.3.2 WEB漏洞类别
振動成	版本	20230417151610			4.4 漏洞排名
2 2 64					4.4.2 WEB漏洞TOP10
2.2 19X3			(21 人资本		5 弱口令
φ.)		加工 [21] 种歌剧病口或服务,开放暖多的病口为 [137] 病口,对应	[2] 1°ær,	吴(4)南元山下龙(hī元)。	6 历史检测详情
序号	病日	100分	MAX TOO	土切	7 参考标准 7 1 单一混调团除单码证中4-4
1	21	Itp	ICP	172.20.50.203	7.2 资产风险等级评定标准
2	22	ssh/WeOnlyDo sshd 2.4.3	ICP	172.20.50.203	8 安全建议
3	23	telnet/Microsoft Windows XP telnetd	TCP	172.20.50.203	9 联系我们
4	80	http/Microsoft HTTPAPI httpd 2.0	TCP	172.20.50.203	_
5	135	msrpc/Microsoft Windows RPC	TCP	172.20.50.203	_
6	137	netbios-ns	TCP	172.20.50.203	
7	137	netbios-ns/Microsoft Windows netbios-ns	UDP	172.20.50.203	
8	139	netbios-ssn/Microsoft Windows netbios-ssn	TCP	172.20.50.203	
9	443	https/apache:http_server:2.4.46 Apache httpd	TCP	172.20.50.203	
10	445	microsoft-ds/Microsoft Windows 7 - 10 microsoft-ds	TCP	172.20.50.203	
11	1433	ms-sql-s/microsoft:sql_server:2008_r2:gold Microsoft SQL Server 2008 R2	TCP	172.20.50.203	
12	1521	oracle-tns/Oracle TNS	ТСР	172.20.50.203	
13	3306	mysql/mysql:mysql:5.6.50 MySQL	ТСР	172.20.50.203	
14	3389	ms-wbt-server/TLSv1	TCP	172.20.50.203	
15	5432	postgresql/postgresql:postgresql:9.6 PostgreSQL DB	TCP	172.20.50.203	
16	5466	http	TCP	172.20.50.203	
17	5677	http	TCP	172.20.50.203	
18	7756	http	TCP	172.20.50.203	
19	8080	http/apache:http_server:2.4.46 Apache httpd	TCP	172.20.50.203	
20	8088	http	TCP	172.20.50.203	
21	56777	http	TCP	172 20 50 203	

21 30777 mtp 说明: 動感端门/服务標標提安全研究表明, 空景被墨客利用漂洞发起攻击的端门/服务。



羚见数据安全检查工具箱用户手册

2.3 电风机	张中间 件			
本次	(任务检测到以下种敏感中间件,	其中使用最多的中间件是【】,具体情况如下表所示:		目录
席号	中间件	网站		1 检测结果综述
2HoF	, 教育中间休息授办会现交主明			2 任务总体概题
17544	1: 或感中间冲走相交主则为浓吻	,各物物类各利用发起攻击的中间件。		2.1 任务基本信息
3 密产	信息统计			2.2 敏感端口/服务
- ~~				2.3 歌歌中间冲
3.1 端[口/服务统计			3.1 端口/服务统计
资产	的端口/服务开放情况如下表所示	R,开放端口最多的资产为【172.20.50.203】,共开放了【45】个端口:		3.2 资产风险等级
序号	主机名	端口/"服务"/协议	端口总数	3.2.1 主机资产风险
1	172.20.50.203	21/"ftp"/"TCP"	45	3.2.2 WEB资产风险
		22/"ssh/WeOnlyDo sshd 2.4.3"/"TCP"		4 漏洞信息统计
		23/"telnet/Microsoft Windows XP telnetd "/"TCP"		4.1.1 系统温洞影响资产
		80/"http/Microsoft HTTPAPI httpd 2.0"/"TCP"		4.1.2 WEB漏洞影响资产
		135/"msrpc/Microsoft Windows RPC "/"TCP"		4.2 漏洞等级分布
		137/"netbios-ns"/"TCP"		4.3 漏洞类别统计
		137/"netbios-ns/Microsoft Windows netbios-ns "/"UDP"		4.3.1 系统漏洞类别
		139/"netbios-ssn/Microsoft Windows netbios-ssn "/"TCP"		4.4 漏洞排名
		443/"https/apache:http_server:2.4.46 Apache httpd"/"TCP"		4.4.1 系统漏洞TOP10
		445/"microsoft-ds/Microsoft Windows 7 - 10 microsoft-ds */"TCP"		4.4.2 WEB漏洞TOP10
		1025/"msrpc/Microsoft Windows RPC "/"TCP"		5 踢口令
		1026/"LSA-or-nterm"/"TCP"		6 历史检测评情 7 急速的 使
		1027/"msrpc/Microsoft Windows RPC "/"TCP"		7.1 单一漏洞风险等级评定标准
		1028/"unknown"/"TCP"		7.2 资产风险等级评定标准
		1048/"neod2"/"TCP"		8 安全建议
		1070/" amrupdateserv"/"TCP"		9 联系我们
		1074/"warmspotMamt"/"TCP"		
		1128/"saphostctrl"/"TCP"		
		1136/"hhb-gateway"/"TCP"		
		1433/"ms-sql-s/microsoft:sql server:2008 r2:gold Microsoft SQL Server 2008 R2"/"TCP"		
		1468/"csdm"/"TCP"		
		1521/"oracle-tns/Oracle TNS "/"TCP"		
		2383/"ms-olap4"/"TCP"		
		3300/"ceph"/"TCP"		
		3306/"mysql/mysql:mysql:5.6.50 MySQL"/"TCP"		
		3389/"ms-wbt-server/TLSv1 "/"TCP"		
		3638/"ehp-backup"/"TCP"		
		5357/"http/Microsoft HTTPAPI httpd 2.0"/"TCP"		
		5432/"postgresgl/postgresgl:postgresgl:9.6 PostgreSQL DB"/"TCP"		
		5466/"http"/"TCP"		
		5500/" oracle/https/oracle:database_server:::enterprise Oracle XML DB Enterprise Edition httpd"/"TCP"		
		5677/"http"/"TCP"		
		5985/"http/Microsoft HTTPAPI httpd 2.0"/"TCP"		
		7756/"http"/"TCP"		
		8000/"http/apache:http_server:2.2.8 Apache httpd"/"TCP"		
		8080/"http/apache:http_server:2.4.46 Apache httpd"/"TCP"		



羚见数据安全检查工具箱用户手册

日录





55.8%I	间资立统计			
.1.1 影响	wsなインルト」 系统-羅同影响资产 主机茨产最多的漏洞是 [Adobe Shockwave Player 環冲区错误漏洞(CVE-2	011-2124) 】,共有【1] 主机中存在该漏洞,漏洞等级力离风险,漏洞影响资产数量TOP10分布如下图	2 任务基本信息 2.1 任务基本信息 2.2 敏感共口/服务 2.3 敏感中间件
	3	洞影响资产数量 Top10		3 资产信息统计
	Addre Stockwein, Apache Gormosi, Apache HTT Se. Apache HTT Se. Apache HTT Se. Apache HTT Se. Apache HTT Se. Apache HTT Se. Apache HTT Se.	1 1 1 1 1 1 1 1 1		 3.1 端口/服务统计 3.2 资产风险等级 3.2 1 生机资产风险 3.2.2 WEB资产风险 4 漏周信息统计 4.1 受影响资产统计 4.1.4 受影响资产统计 4.1.4 系统漏洞影响资产 4.2. WEB漏洞影响资产 4.2 服洞爆吸分布
系统	漏洞影响主机资产数量TOP10如下表新示。	1		 4.3 編列契約時以下 4.3.1 系统漏洞处則 4.3.2 WEB漏別使則 4.4 漏洞排名 4.4 漏洞排名 4.4.1 系统漏洞TOP10 4.4.2 WEB漏洞TOP10 5 認口会
号	「漏洞名称」	漏洞分组	受影响资产	6 历史检测详情
	Adobe Shockwave Player 缓冲区错误漏洞 (CVE-2011-2124)	缓冲区溢出	172.20.50.203	7 参考标准
	Apache Commons Configuration 和人验让错误漏洞(CVE-2020-1953) 輸入短止	172,20,50,203	7.1 単一漏洞风险等级评定板
	Apache HTTP Server httpoxy 安全漏洞 (CVE-2016-5387)	いりが空制	172.20.50.203	8 安全建议
	Apache HTTP Server 代码问题满词 (CVE-2021-26690)	代码问题	172.20.50.203	9 联系我们
	Apache HTTP Server 代码问题漏洞 (CVE-2021-34798)	代码问题	172.20.50.203	
	Apache HTTP Server 代码问题漏洞(CVE-2021-44224)	代码问题	1/2.20.50.203	
	Apache HTTP Server 信息泄露漏洞 (CVE-2022-30556)	信息泄露	172.20.50.203	
	Apache HTTP Server 安全漏洞(CVE-2016-8743)	代码问题	172.20.50.203	
	Apache HTTP Server 安全漏洞(CVE-2021-33193)	長日	172.20.50.203	
1.2 ' 影响	WEB漏洞影响资产 Web资产最多的漏洞是【HTTP Referrer-Policy头缺失】,共有【16】个Web HTTP Referrer	站点中存在该展问, 漏洞 洞影响进产数量 Top10 16 16 16 16 15	等级为【低风险】。漏洞影测资产数量TOP10分布如下图所示:	







羚见数据安全检查工具箱用户手册

(intro)					日录
4.4.1 按漏	系统漏洞TOP10 洞名称排序,系统漏洞发现次数TOP10分布情况如下图所示:				1 检测结果综述 2 任务总体概览
		漏洞排名 Top10			2.1 任务基本信息
	HTTPRe应头X-Conte	1	1		2.2 敏感端口/服务
	HTTP吨应头使用X-XSS HTTPI吨应头型研用X-Fr	16			2.3 戰/感中间件 3 溶充信自体注
	HTTP安全返回头Stric	16			3.1 端口/服务统计
	Apache HTTP Se	16			3.2 资产风险等级
	Apache HTTP Se Apache HTTP Se	16			3.2.1 主机资产风险
	Apache HTTP Se	3			3.2.2 WEB资产风险
		3			4 漏洞信息统计
		3			4.1 受影响资产统计
		3			4.1.1 系统满问影响资产 4.1.2 M/D 是词影响发车
		3			4.1.2 WEB周州夏州页
		3			4.3 漏洞类别统计
		0	1 10		4.3.1 系统漏洞类别
系统	漏洞出现次数TOP10如下表所示:				4.3.2 WEB漏洞类别
号	系统漏洞名称		漏洞分组	总计 (次)	4.4.1 系统漏洞TOP10
	▲HTTP响应头X-Content-Options: nosniff检查		默认探测	16	4.4.2 WEB漏洞TOP10
	▲HTTP响应头使用X-XSS-Protection检查		默认探测	16	5 弱山令 6 历史检测详情
	▲HTTP响应头部使用X-Frame-Options检查		默认探测	16	7 参考标准
	▲HTTP安全返回头Strict-Transport-Security检查		默认探测	16	7.1 单一漏洞风险等级评定标
	Apache HTTP Server 代码问题漏洞(CVE-2021-34798)		代码问题	3	7.2 资产风险等级评定标准 8 安全建议
	Apache HTTP Server 信息泄露漏洞 (CVE-2022-30556)		信息泄露	3	9 联系我们
	Apache HTTP Server 数据伪造问题漏洞(CVE-2022-31813)		数据伪造	3	
	Apache HTTP Server 环境问题漏洞(CVE-2022-22720)		环境条件	3	
	Apache HTTP Server 缓冲区错误漏洞 (CVE-2021-39275)		缓冲区溢出	3	
)	Apache HTTP Server 缓冲区错误漏洞(CVE-2021-44790)		缓冲区溢出	3	
按漏	源名物由序,Web漏测发现次数TOP10分布情况如下图所示:	編測相名 Top10 101 73 71 60 21 20 20 16 16			
Web	p漏洞出现次数TOP10如下表所示:	0 10 20 30 40 36	00 70 80 10 100	614 (M)	
	AM 1907 1500		14.1.53	#311 178 J	



5 弱口令						目录	
序号 主机地	由址	用户名	密码	服务	端口	1 检测结果综述 2 任务总体概览	
6 历史检测详	情					2.1 任务基本信息 2.2 敏感端口/服务	
本次任务历史	14 15 16 16 17 17 17 17 17 17 17 17	Con Sec. 1	■ ₩63第334数	50 		2.3 敏感中间体 3 波洋信息统计 3.1 海口/服务统计 3.2 波产风险等级 3.2.1 主机波产风险 3.2 以TE数学元风险 3.2 以EB数产风险 4.周信息统计 4.1 复彩陶瓷产统计 4.1 系统晶形影响波产 4.1 系统晶形影响波产 4.2 漏洞每级分布 4.3 漏洞规则线计 4.3 系统漏洞规则 4.3 系统漏洞规则 4.3 系统漏洞规则 4.3 系统漏洞规则 4.3 系统漏洞规则 5.3 同口令 6 匹由於的副對標	
具体历史检测	则时间段及漏洞结果总计如下表所	र्गच्छः:				7 参考标准	
任务类型	开始时间		结束时间		漏洞总计	7.1 平一浦河风应粤极评定标准 7.2 资产风险等级评定标准	
系统扫描	2023-05-06 15:43:18		2023-05-06 16:01:14		897	8 安全建议	
弱口会扫描	2023-05-06 16:01:21		2023-05-06 16:30:55		0	9 联系我们	
WEB扫描	2023-05-06 16:01:21		2023-05-06 17:24:29		501		
7 会北行准							
7 参考标准 7.1 单—漏洞风	1.险等级评完标准						
危险程度	危险值区域	危险程度说明					
▲高	7 <= 漏洞风险值 <= 10	攻击者可以访问机密信息、破坏或删	除数据且可以制造系统中断。				
A #	4 <= 漏洞风险值 < 7	攻击者可访问部分受限的信息。可以	破坏信息日可以禁用网络中的个体目标	雨系统。			
	0、海河风险值、1	(人生音)(5)(5)(5)(5)(5)(5)(5)(5)(5)(5)(5)(5)(5)	的信息 破坏武堤坏信息归于注制法的	1.何亥徐山斯			
		次出当可以住1974間の150197500	19]급·조·, 베이카이데아카이급·조·1드가니/Ample1.	T In 2000 C T WILe			
2. 目标系统 3. 可远程短期 5. 可远程和期 6. 可远程和期 7. 可远程规辑 9. 可远程以转 9. 可远程以转 10. 可远程型 7.2 资产风险 等	报發器开放了不必要的服务。 句別屬進不在目录附中的文件疏 为全然言理的问题等身份目示, 用受影响的系统服务器攻击其他 和系统文件或后台数据集。 雪透和户身份执行命令(变現, 習透和户身份执行命令(变現, 習透和户身份执行命令(灭現。 習透和户身份执行命令(不受現。 約別存示式	表取服务器动击脚本的原码。 加速网站的用户。 色服务攻击。 不太雪易利用)。 驾易利用)。					
带产风险墨纳	带产MB	の伯区間					
10. 可远程以信 7.2 资产风险等	5堆用户身份执行命令(不变限、 1级评定标准	容易利用)。				4.4 漏洞排名	
资产风险等级	资产风险	全值区域				4.4.2 WEB漏洞TOP10	
0非常危险	8 <= 资	产风险值 <= 10				5 弱口令	
0 比较危险	5 <= 资	产风险值 < 8				6 历史检测详情	
0 比较安全	2 <= 资	浐风险值 < 5				7 参考标准 7 1 单_课源网际给领国由生业	
◎ 非常安全	0 <= 资	产风险值 < 2				7.1 单一漏洞风运奏级计定标准 7.2 资产风险等级证完标准	
1. 将资产的源 2. 单个资产的 3. 高、中、伯 4. 资产的风险	高洞按照分数的高低排序,依摄测 的风险值按照风险评估模型计算系 武漏洞威胁的定义参见《单一漏测 全等级定位为四级;非常危险、b	漏洞的分数将漏洞威胁划分为高、中、低 未得到;网络的风险值是由最危险资产; 同风险等级评定标准》。 七较危险、比较安全和非常安全。具体的	6三个类别。 9定,即最大的资产风险值。 9评判标准请参考《资产风险等级评定	标准》。		7 1 20 / Margarovi / 2000 8 安全建议 9 联系我们	
8 安全建议							
随著越来越多的闪绕访问通过系统漏测进行操作、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看和系统用户的安全,我们有必要采取措施调除这些风险。 建议对存在漏隙的资产参考例件中提出的解决方案进行漏洞停补、安全撤强。 请专业的安全研究人员进行安全编码方面的安全间的安全审计,修补所有发现的安全漏洞,这种白盘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,在开发过程是金属洞的时人都经到事中功倍的效果。 采用专业的系统安全产品,可以在不像改系统本格的情况下对大多数的基于漏洞攻击起到事中功倍的效果。 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,特别显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 确及对系取措施。							
9 联系我们							
公司: 熙羚信 网址: https:, 热线: 0571-4 传真: suppo 地址: 浙江省	建技术有限公司 //www.xilinginfo.com/ 86955515 rtd@seclead.cn 杭州市演江区长河街道演集路3	52号中控信息大厦82505					

图 9.2.3.1-1 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。



9.2.3.2 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:

							1 检测结果综述		
1 检测结果综计	2 资产总体概览								
十次招告中	2.1 资产基本信息								
本/大扳百甲, 数/大风险/高升	本以按言中, 击线 [17.2.0.34.240] 并短期间规范237, 其于基础漏削237, WeD属用(27), 就可受UT。 数字目的医治1.0								
《资产风险等级评	国体外にはロジンの、医士学なりで「十日内にない」、所有期間中に、同時期間中で、中国期間ので、住宅期間ので、住宅地間ので、住宅が加速すなはガス大規制及其广次経営なガス大規則、情勢以至す (後午风除金はが平時代書)、								
							3 资产端口服务信息		
2 资产总体概	览						4 主机漏洞信息		
21资产基本信	白						4.1 主机漏洞统计概况		
	=						4.1.1) 馮河等級分布 112) 震潮発明(会社		
系统实际列表	衣:						4.1.3 漏洞排名		
							4.2 主机漏洞详情		
主机名称	172.20.54.246						5 WEB漏洞信息		
主机资产	172.20.54.246						5.1 WEB漏洞统计概况		
操作系统	FreeBSD 7.0-RELE	ASE-p1 - 10.0-CUF	RENT				5.1.1 漏洞等级分布		
MAC地址							5.1.3 漏洞排名		
扫描时间	系统扫描: 开始时	间: 2023-05-08 14	:48:42 至 2023-05-08 14:55:0	01(耗时: 6分19秒)			5.2 WEB漏洞详情		
资产风险值	9.8						6 弱口令		
漏洞分布	漏洞总计: 23						7 参考标准 7 1 单		
	高风险: 9						7.2 资产风险等级评定标准		
	中风险: 5						8 安全建议		
	低风险:5						9 联系我们		
	信息风险: 4								
漏洞状态标识	新増: 23								
	误报: 0								
	已修复: 0								
资产组	默认资产组								
标签									
系统版本	V3.0(6.6.1-R1-v90	1757-20230222)							
规则库版本	20230324144746								
WEB资产列表	表:								
22款休湿调饼	6 11								
大招告中有4	今 [1] 个主机资产 法主机由	友在 [0] 个Wabt	占 财主机和Wab进行整体混	司会析的情况加下事所示 土机和Wabi	关细湿洞信息口查节/	會节5			
		E IOI I WEDE	m, x) ± 0 010 000001 0 ± 040m	14 10/07/010318/02/2017-22/07/07/2017	+知順的同志の早 ()+。 信白	白 井			
TF/ORL THE		0	5	5	100.22	22			
WEB:居词		0	0	0	-	0			
中 计		9	5	5	4	23			
23 敏感端口/	服名		-						
本次任务培训	副到开放了以下「2」、种数成時	口或服务 目休病源	如下表新示·						
(中央)(1312)(A)	端口		肥久		1013V				
18-5	3 1		Rbc5	du ant rovio lu l	TCD				
	80		vmware esxi serve	er/nttp/vWware ESXi Server httpd	ICP				



本次任务检测到以下 [0] 种敏感中间件,具体情况如下表所示: 序号 中间件 说明: 敏感中间件是指安全研究表明, 容易被黑客利用发起攻击的中间件。 3 资产端口服务信息 资产的端口/服务开放情况如下表所示,共开放了【7】个端口: 端口 协议 漏洞总数 服务 ⊞ 80 vmware esxi server/http/VMware ESXi Server httpd тср 5 427 svrloc/Service Location Protocol 2 UDP 0 ⊞ 443 TCP https 16 тср ⊞ 902 iss-realsecure/VMware Authentication Daemon 1.10 1 тср 8000 http-alt 0 8300 тср tmi 0 9080 soap/genivia:gsoap:2.8 gSOAP TCP 0 ICMP H --1

高风险

9

4 主机漏洞信息

2.4 敏感中间件

4.1 主机漏洞统计概况



序号	主机漏洞类别 (TOP10)	总计
1	跨站脚本	14
2	默认探测	7
3	其它	1
4	Wab成田	1

低风险信息级

4

总计

23

中风险

5

5

目录
1 检测结果综述
2 资产总体概览
2.1 资产基本信息
2.2 整体漏洞统计
2.3 敏感端口/服务
2.4 敏感中间件
3 资产端口服务信息
4 主机漏洞信息
4.1 主机漏洞统计概况
4.1.1 漏洞等级分布
4.1.2 漏洞类别统计
4.1.3 漏洞排名
4.2 主机漏洞详情
5 WEB漏洞信息
5.1 WEB漏洞统计概况
5.1.1 漏洞等级分布
5.1.2 漏洞类别统计
5.1.3 漏洞排名
5.2 WEB漏洞详情
6 弱口令
7 参考标准
7.1 单一漏洞风险等级评定标准
7.2 资产风险等级评定标准
8 安全建议
9 联系我们

版权所有 © 领信数科



					目录
4.1.3	屬洞排名				1 检测结果综述
		漏洞排名 Top10			2 资产总体概览
	Vikware ESG 跨达				 2.1 资产基本信息 3.2 乾片浸渍法
	Viliviare ESXI 安全	1			2.3 敏感法□/服务
	Vitivare ESXI #EP	1			2.4 敏感中间件
	Vieware ESO PER	1			3 资产端口服务信息
	Vinware Cloud F	1			4 主机漏洞信息
	Vitware ESXI, Wo	1			4.1 主机漏洞统计概况
		1			4.1.1 馮洞等取分布 4.1.2 深泻类剧体计
		1			4.1.3 漏洞共为的01
		1			4.2 主机漏洞详情
		1			5 WEB漏洞信息
		0			5.1 WEB漏洞统计概况 5.1.1 漏洞等级分布
序号	系统漏洞名称 (TOP10)			总计	5.1.2 漏洞类别统计 5.1.3 漏洞排名
1	▲ VMware ESXi 跨站脚本漏洞(CVE-2020-3955)			1	5.2 WEB漏洞详情
2	▲ VMware ESXi 资源管理错误漏洞(CVE-2020-4004)			1	6 弱口令
3	▲ VMware ESXi 安全漏洞(CVE-2020-4005)			1	7 多考你准 7 1 单一漏洞风险等级评完标准
4	▲ 威睿 VMware ESXi 缓冲区错误漏洞(CVE-2021-21974)			1	7.2 资产风险等级评定标准
5	▲ VMware ESXi 缓冲区错误漏洞(CVE-2021-21995)			1	8 安全建议
6	▲ VMware ESXi 授权问题漏洞(CVE-2021-21994)			1	9 联系我们
7	▲ Vmware Cloud Foundation 资源管理错误漏洞(CVE-2021-22	2050)		1	
8	▲ Vmware Cloud Foundation 输入验证错误漏洞(CVE-2021-22	2043)		1	
9	▲ VMWare Cloud Foundation (ESXi) 访问控制错误漏洞 (CVE-2	2021-22042)		1	
10	🔺 VMware ESXi、Workstation和Fusion 安全漏洞(CVE-2018-6	5972)		1	
4.2 主机源	新洞 详情				
漏洞名称		漏洞分类	漏洞类型	出现次数	
	Mware ESXi 跨站脚本漏洞(CVE-2020-3955)	跨站脚本	高风险	1	
	ware ESXi 资源管理错误漏洞(CVE-2020-4004)	资源管理错误	高风险	1	
	Mware ESXi 安全漏洞(CVE-2020-4005)	其它	高风险	1	
田 🔺 威	書 VMware ESXi 缓冲区错误漏洞(CVE-2021-21974)	缓冲区溢出	高风险	1	
	Mware ESXi 缓冲区错误漏洞(CVE-2021-21995)	缓冲区溢出	高风险	1	
	Mware ESXi 授权问题漏洞(CVE-2021-21994)	授权问题	高风险	1	
🗄 🔺 Vn	nware Cloud Foundation 资源管理错误漏洞(CVE-2021-22050)	资源管理错误	高风险	1	
🗄 🔺 Vn	nware Cloud Foundation 输入验证错误漏洞(CVE-2021-22043)	輸入验证	高风险	1	
	/Ware Cloud Foundation (ESXi) 访问控制错误漏洞(CVE-2021-2204	2) 访问控制	高风险	1	
	Aware ESXi、Workstation和Fusion 安全漏洞(CVE-2018-6972)	代码问题	中风险	1	
E 🔺 🎉	款Intel产品信息泄露漏洞(CVE-2018-3646)	信息泄露	中风险	1	L
🗉 🔺 VN	Mware ESXi 资源管理错误漏洞 (CVE-2020-3976)	资源管理错误	中风险	1	



5.1 WEB漏洞统计概况							Pa
5.1.1 漏洞等级分布							1 检测结果综述
		高风险	中风险	低风险	信息级	总计	2 资产总体概览
		0 0 0				0	2.1 资产基本信息
							2.2 整体漏洞统计
							2.3 歌/函师山/服务 2.4 敏感血间/性
							3 资产端口服务信息
							4 主机漏洞信息
							4.1 主机漏洞统计概况
							4.1.1 漏洞等级分布
							4.1.2 漏洞突别统计 4.1.2 漏洞突别统计
							4.2 主机漏洞详情
							5 WEB漏洞信息
							5.1 WEB漏洞统计概况
							5.1.1 漏洞等级分布
							5.1.2 漏洞类别统计 5.1.2 漏洞类名
5.1.2 漏洞类别统计							5.2 WEB漂河详信
		应号 W	FB深洞类别			总计	6 弱口令
		12.2				-541	7 参考标准
							7.1 单一漏洞风险等级评定标准
							7.2 资产风险等级评定标准 8 去全建议
							9 联系我们
5.1.3 漏洞排名							
序号 WEB漏洞名称 (TOP10)					总计		
5.2 WEB漏洞详情							
漏洞名称		漏	洞分类		漏洞类型	出现次数	
5 弱口令							
序号 王机地址	用户名	密码	56	()	端口		



7参考标准			目录
7144 18101			1 检测结果综述
7.1 单一满洞。	风险寺奴许定的旧		2 资产总体概览
危险程度	危险值区域	危险程度说明	2.1 资产基本信息
	7 <= 漏洞风险值 <= 10	攻击者可以访问机密信息,破坏或删除数据日可以制造系统中断。	2.2 登体漏洞统计
			2.3 電影感情以/服装
- #	4 <= 1約/円/八印空1目 < 7	以正言可加问的方式就到1日志、可以吸水日志且可以表出网络中的17月4日的金额。	2.4 或数下间中 2. 将产油口服冬信自
▲ 低	0 < 漏洞风险值 < 4	攻击者可以在特殊情况下访问不受限的信息、破坏或损坏信息但无法制造任何系统中断。	4 主机源洞信息
▲ 信息	漏洞风险值 = 0	攻击者可以获取服务及组件等版本信息。	4.1 主机漏洞统计概况
1.可远程 2.目标 3.可远程程程 5.可远程程程 8.可远远程程 8.可远远程程 9.可远远程程 9.可远远程程 9.可远远程程 9. 0.可远程程 9. 0.可远程程 9. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.	和減調的維約版本信息。 結腸等發行数プ不必要的服务。 制服等發行数プ不必要的服务。 用受影响的注意的可觀导致最合置用 用受影响的注意的容量, 有差统文件、還作后台数据集。 這週用戶書的代行命令或进行行命令就 后還理用戶書的代行命令(發展、 這理理戶目書的代方命令(發展、 這要用戶書的代方命令(受現、 這要用戶書的代方命令(读取服务器动态越本的源码。 。 浏览网站的用户。 "绝服务攻击。 不太驾影利用)。 、容易利用)。	 4.1.1 國同等級分布 4.1.2 國同美則統計 4.3 國同非路 4.2 主机屬同時備 5 WEB屬同結局 5.1 WEB屬同結局 5.1 WEB屬同族計斷況 5.1.2 獨同美則統計 5.3.3 國同非名 5.2 WEB屬同律債
资产风险等级	资产风	险值区域	6 弱口令 7 条考标准
3 非常危险	8 <= 3	资产风险值 <= 10	7.1 单一漏洞风险等级评定标准
0 比較危险	5 <= 3	<u> 资产风险值 < 8</u>	7.2 资产风险等级评定标准
0 比較安全	2 <= 3	资产风险值 < 5	 安主建议 9 联系我们
◎ 非常安全	0 <= 3	<u>贫产风险值 < 2</u>	
1. 將资产的 2. 单个资产 3. 高、中、 4. 资产的风	5漏洞按照分数的高低非序,依据 F的风险值按照风险评估模型计算 低漏洞威胁的定义参见《单一漏 风险等级定位为四级;非常危险、	漏陶的分数体漏现或助力分离。中、低二个类别。 涞喝到: 网络的风险值量由最危险资产决定,即最大的资产风险值。 洞风耸垂取汗走际步)。 比较危险、比较安全和非常安全。具体的评判际准请参考《资产风险等级评定际准》。	
8 安全建议			
随着越来越 统管理者和系统 建议对存在 请专业的安 对系统的开 采用专业的 建议网络答 响及时采取措施	容的网络访问通过系统漏原进行 用户的安全,我们有必要采取错 漏原的资产参考附件中理出的解 全研究人员或安全公司对系统架 发人员进行安全编网方面的培训 提及人员进行安全编码方面的培训 提及、系统管理员、安全管理员 。	晶作。系统黑脚已成为互联网安全的一个热点,甚于系统黑脚的攻击广为流行,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 被消除这些风险。 夫方套进行黑眼倾补、安全错强。 也做全面的安全审计,修补所有发现的安全黑闹,这种白盒安全测试比较深入全面。 在开发过程金龟黑胸的引入地起到事中功倍的效果。 抗去身的情不下对大多数的基于漏洞攻击起到有效的短断作用。 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	
9 联系我们			
公司: 熙羚 网址: http 热线: 0571 传真: supp 地址: 浙江	信息技术有限公司 is://www.xilinginfo.com/ 1-86955515 port@seclead.cn 省杭州市滨江区长河街道滨康路:	352号中控信息大厦82505	



9.2.4 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。

9.2.4.1 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:



新增报表模板					×
报表模板名称			* 报表模板名	3称,长度在[4-16]之间	
漏洞等级	✔ 高风险	✓中风险	✔低风险	✔信息	
漏洞状态	✔ 新増	✔ 误报	✓已修复		
是否导出检测详情	×				
自定义公司信息	×				
报表标题	漏洞扫描安全评估	报告	*提示:限制	副: [4-30]字符之间;	
	1		收 前子 付:(@\$%^&{}=/^? <>\ :	
自定义报表章节	×		* 提示: 自知	定义报表章节仅限[html/pdf]报表且不支持基线任务。	
	提交				

图 9.2.4.1-1 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

▲ 导出报表	表 ,报表模板		
輸出报表			
选择导出模式	 按任务 按资产 		
任务名称	请选择任务		*提示: 请选择需要导出的任务 (支持多选, 不支持存活任务)
計出格式	🖲 HTML 🕤 🛛 WORD W 📿 PDF	C EXCEL 🔀 🔿 XML 📶	*提示:包含基线任务时,不可导出PDF格式
即出方式	详细报表	▼ *提示: 请选择导出方式。基线任务仅支持统计报表导	н
出文件名		*提示: 请填写导出的文件名称。限制: [1-42]字符之间	旬,限制字符: /**<>│()`{}&;\$:?
置压缩包密码	×		
否展示弱口令密码	~		
表模板	默认模板	▲ *提示:请选择报表模板	
	默认模板		
导出	报表模板0426		
	报表模板0506		

图 9.2.4.1-2 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:



机咱权农民权		
报表模板名称		* 报表模板名称,长度在[4-16]之间
1000 DE IX HITT		
漏洞等级	✓ 高风险	
漏洞状态	✔新増 ✔误报	✓已修复
是否导出检测详情	×	
自定义公司信息	×	
报表标题	漏洞扫描安全评估报告	*提示:限制:[4-30]字符之间;
		限制字符: @ \$ % ^ & {} = / * ? * < > \ :
自定义报表章节	×	*提示:自定义报表章节仅限[html/pdf]报表且不支持基线任务。
	统计报表章节自定义	详细报表章节自定义
	☑1 检测结果综述	☑1 检测结果综述
	□ 2 任务总体概览	□ 2 资产总体概览
	☑ 2.1 任务基本信息	☑ 2.1 资产基本信息
	☑ 2.2 敏感端□/服务	☑ 2.2 整体漏洞统计
	☑ 2.3 敏感中间件	☑ 2.3 敏感端口/服务
	□ 2 资产信息统计	☑ 2.4 敏感中间件
	☑ 3.1 端口/服务统计	☑ 3 资产端口服务信息
	□ 🕑 3.2 资产风险等级	□ 🗹 4 主机漏洞信息
	☑ 3.2.1 主机资产风险	□ 🖸 4.1 主机漏洞统计概况
	☑ 3.2.2 WEB资产风险	☑ 4.1.1 漏洞等级分布
	□ 🗹 4 漏洞信息统计	☑ 4.1.2 漏洞类别统计
	□	☑ 4.1.3 漏洞排名
	☑ 4.1.1 系统漏洞影响资产	☑ 4.2 主机漏洞详情
	☑ 4.1.2 WEB漏洞影响资产	□
	☑ 4.2 漏洞等级分布	□
		☑ 5.1.1 漏洞等级分布
	☑ 4.3.1 系统漏洞类别	☑ 5.1.2 漏洞类别统计
	☑ 4.3.2 WEB漏洞类别	☑ 5.1.3 漏洞排名
	- 4.4 漏洞排名	☑ 5.2 Web漏洞详情
	☑ 4.4.1 系统漏洞TOP10	☑ 6 弱□令
	☑ 4.4.2 WEB漏洞TOP10	
	☑ 5 弱□令	☑ 7.1 单一漏洞风险等级评定标准
	◎ 6 历史检测详情	☑ 7.2 资产风险等级评定标准
	- 🖸 7 参考标准	◎ 8 安全建议
	☑ 7.1 单一漏洞风险等级评定标准	☑ 9 联系我们
	☑ 7.2 资产风险等级评定标准	
	☑ 8 安全建议	
	☑ 9 联系我们	
	提交	

图 9.2.4.1-3 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



▲ 导出报表 12 报表列表 ▲	报表模板		
输出报表			
选择导出模式	 接任务 按资产 		
任务名称	请选择任务		*提示:请选择需要导出的任务(支持多选,不支持存活任务)
导出格式	💿 HTML 🕤 🛛 WORD 📝 📿 PDF 📐	O EXCEL 🔀 🛛 XML 🚾	*提示:包含基线任务时,不可导出PDF格式
导出方式	详细报表 ▼	*提示:请选择导出方式。基线任务仅支持统计报表导出	
导出文件名		*提示:请填写导出的文件名称。限制: [1-42]字符之间,限制	字符: / \ * " < > () ` { } & ; \$: ?
设置压缩包密码	×		
是否展示弱口令密码	~		
报表模板	test-自定义报表章节 ▼	* 提示: 请选择报表模板	
會田			

图 9.2.4.1-4 选择自定义报表章节导出

9.2.4.2 报表模板操作

管理员可以对报表模板中的信息进行编辑和删除操作。

≽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

9.3 流量探测报告导出

WEBUI: 主界面 -> 报告中心 ->流量探测报告导出

流量探测报告导出可导出流量探测界面的所有列表内容,报告可根据探测类型、探测时间、是否安全进行筛选。导出完成后,下方历史导出记录同步新增一条导出记录。

			0.5458			
-		WITH U AMONG C KININA C CAMALA C DISANG	O SMATH			
al of the						
92	新建导出任务					
19490	·#850 0200					
	NUR2 28 · · · ·	100 20 · · · · · · · · · · · · · · · · ·	(u)			
	5/219:0 II II					
	医中口中记录					
		10000	10 mars	874-10-mail	84	
		C*	12.95%	2014-01-10 1049-01		
		nogen-	Gade	2024-01-13 10 39 54		
		24503-941	Rame	2024-01-14 10 1108	873	
		22G899	Setter.	2023-11-15 15:12:04		
		dans-ng Gaas	Gates	2025-11-07 10-20 19		
	6	成保定和法律研究研究	Ratin	2023-10-16 10-80/15	Bitt	
	¥.	元编学名	探测预测	2028-10-12 (107ka)	872	
		test-den	Harris	2023-09-19-07-22-13		
		2P1	探击然逝	2023-08-18 1911-25	802	
	10	mysa#3##35	PATES .	2023-09-12 1747-25	影技	
					BUTTE (

图 9.3 流量探测报告导出



十. 系统配置

系统配置目前当前只有系统监控页面。

10.1 系统状态

系统状态页面,展示设备信息、运行状态、CPU/内存/交换分区使用率、版本号等信息。



10.2 报告输出配置

KAFKA 输出:可以配置 KAFKA 地址,将部分数据推送过去。

	◎ 资产管理					
ta.	③ 新時記書 / H 報告輸出配置					
e:::RZE	і кағқа輸出					
	KAFKABE	topic	是否启用		un .	
	172.20.57.71:19092	disTopic	后用	v	测试 保存配置 删除	
	172.20.57.219:19092	disTopic	加用	v	测试 保存配置 删除	
	172.20.66.14:19092	disTopic	后用	v	測试 保存配置 删除	
	172.20.52.230:19092	dis Topic	無用	v	對试 保存配置 删除	
	172.20.57.51:19092	testTopic	業用	Ŷ	將武 保存配置 删除	
	172.20.57.56:19092	testTopic	前用	×	務試 保存配置 删除	
	172.20.57.56:19092	testTopic	10.7E)	v	新式 保存配置 撒除	
	172.20.57.5719092	testTopic	启利	v	影试 保存配置 删除	

图 10.2 系统监控

操作:在报告输出配置页面,点击【添加一行】,自动创建后输入 KAFKA 地址、topic、 是否启用。



10.3 出境填报

WEBUI: 主界面 -> 系统配置 ->出境填报

出境填报功能,旨在于解决例如网信办等场景下的出境分析问题。新增的出境数据,根据出境源 IP、出境目的 IP、出境数据白名单、传输条数匹配,敏感数据在条件范围内属于白 名单,可不命中响应的敏感数据模型,超出条数范围/出境数据白名单范围,可在探测告警中 命中出境账实不符模型。

出境源IP	请填写			出境填报人 清填写		出境业务概述	请填写			9、捜索	CI
出境目的IP	请填写			填报时间 开始日期 → 结束日期	8	出境数据白名单	请选择				
										1册修计 +	新增
序号	被检单位	出境源IP	出境填报人	出境业务概述	出境目的IP	出境数据白名	3单	填报时间	传输条数	操作	
1	领信数科12	172.20.57.51	不额度不会	1) DCBOX使用前提:客户待检测的设备,网络环境	172.20.50.145	18位身份证明	昌码	2024-05-29 10:36:19	10000/天	编辑 删除	
2	新东方3	0.0.0.0	渔民更	新电脑官方就阿瑟东;群号五九二反对全微分大户欸	255.255.255.255	手机号(中国)	内地)	2024-05-29 10:37:41	99/小时	编辑 删除	
3	123	172.20.57.51	123	c存在多扫出端口的问题:确认后发现是2501盛邦页	255.255.255.255	银行卡号。座楼	11号码,中国澳门移动电	2024-05-29 13:48:59	1/小时	编辑 删除	
4	test	192.0.0.4	tt		190.0.0.3	座机号码、银行	亍卡号,车架号	2024-06-05 13:19:37	10000/小小时	编辑 删除	
5	领信数科	172.20.57.51	123		172.20.50.145	座机号码		2024-06-05 14:41:11	0/小小时	编辑 删除	
6	123	0.0.00	渔民更		172.20.50.145	18位身份证明	書码	2024-06-05 14:41:32	1/小时	编辑 删除	
7	这是——个直的要验	172.20.50.145	李世民	李世民的手机号是白名单	172,20.54,28	手机局(中国)	(地内	2024-06-05 15:00:50	50///\87	编辑日册除金	

图 10.3 出境填报列表



新增填报				×
* 被检单位	请填写			
* 出境源IP	请填写			
* 出境目的IP	请填写			
* 出境填报人	请填写			
* 出境数据白名单	请选择			\sim
* 传输条数	请填写	- t		
业务概述	请填写			
				<i>i</i>
			取消	确认

图 10.2 新增填报

操作:在填报列表页面,点击"新增填报"按钮,输入被检单位、出境源 IP、出境目的 IP、出境填报人、出境白名单、传输条数、业务概述等信息,点击"确认"。

新增成功会在页面生成对应的填报记录。

10.4 诊断工具

10.4.1 端口探测工具

WEBUI: 主界面 -> 系统配置 -> 诊断工具-> 端口探测工具

进入端口探测工具页面,输入探测 IP/域名,探测端口/范围,点击"探测",可进行 IP



及端口范围的探测。

臣	◎ 资产管理 ◎ 脆弱性核	浏 ☑ 脆弱性模板	교 流星探测	⊙ 敏感探测	◎ 合规检查	☑ 报告中心	◎ 系统配置
■ 系统状态	◎系統配置 / ⊙诊断工具 /	端口探测工具					
⊢ 报告输出配置	* 探测IP/域名						
↑ 出境填报	172.20.66.34 注:限制字符输入:'` \$;\	\n < > / ? : " ()					0
③ 诊断工具 ^	探测端口/范围						
端口探测工具	请填写						
✓ ping工具	请输入探测端口:例:22,80,443 不填入端口内容,默认查找翻 注意:默认探测超时时间为3m	8,8080,20-200。 最有可能开放的1000端口。 iin,超过3min,则退出,同	可能会存在无数据情况	7.			
 Tcpdump工具 	493 Sait						
兴 信息故障收集	17K 201						
	探测端口						
	Г			٦Γ			·
	端口号: 22 服务名称: ssh		端口号: 111 服务名称: rpcbind		端口号: 443 服务名称: htt	ps	端口号: 9009 服务名称: pichat
	L	J L					

图 10.4.1 端口探测工具

10.4.2 Ping 工具

WEBUI: 主界面 -> 系统配置 -> 诊断工具-> ping 工具

进入 ping 工具页面,输入对应的资产 ip 或域名,点击"测试",可进行目标资产的网络扫描检测。

E	◎资产管理	⊙ 脆弱性检测	☑ 脆弱性模板	回 流量探测		◎ 合规检查	☑ 报告中心	◎ 系統配置							
■ 系统状态	◎ 系統配置 / ⊙	◎ 系統配置 / ⊙ 诊断工具 / // ping工具													
₩ 报告输出配置	Ping工具	Ping工具													
↑ 出境填报			* 172.20.66.	34					》 测试						
 ⊙ 诊断工具 ^ 			注:限制字符	夺输入: '` \$;\\n∙	< > / ? : "()										
端口探测工具	PING 172 64 bytes	PING 172.20.66.34 (172.20.66.34) 56(84) bytes of data. 64 bytes from 172.20.66.34: icmp_seq=1 ttl=63 time=0.345 ms													
✓ ping工具	64 bytes 64 bytes 64 bytes	64 bytes from 172.20.66.34; kmp_seq=2 ttl=63 time=0.353 ms 64 bytes from 172.20.65.34; kmp_seq=3 ttl=63 time=0.354 ms 66 bytes from 173.20.65 (incressed = 10.65 time=0.014 ms													
Icpdump工具	172.2	0.66.34 ping statistic	s												
兴 信息故障收集	4 packets rtt min/a	1/2.2Ub6.34 ping statistics 4 packets transmitted, 4 received, 0% packet loss, time 2999ms rtt min/avg/max/mdev = 0.291/0.335/0.354/0.034 ms													

图 10.4.2 ping 工具

10.4.3 Tcpdump 工具

WEBUI: 主界面 -> 系统配置 -> 诊断工具-> Tcpdump 工具

进入 tcpdump 工具页面,选择协议类型、输入相应的数据条目、接口、主机 IP/域名, 点击启动,停止后可下载相应的抓包文件。



Ξ	◎ 资产管理	◎ 脆弱性检测	☑ 脆弱性模板	₩ 流量探測	⊘ 敏感探测	◎ 合規检查	☑ 报告中心	③ 系统配置	
■ 系统状态	◎ 系統配置 / ⊙) 诊断工具 / 🖽 Tepe	lump工具						
⊢ 报告输出配置	Tcpdump	L首							
↑ 出境填报	*协议类型	tcp						\sim	
○ 诊断工具 ^	* 数据条目	100							
端口探测工具		请输入数字,并且在	[1-10000]之间						
一 ping工具	* 接口	eno2						×	
 Tcpdump工具 	* 主机IP/域名	请填写 请输入主机IP/域名。	注意:不分区源、目的	SIP/域名限制字符辅	ì入:'` \$;\\n < >	/?:"()			
·	注意完成配置	后,点击"启动"开始	规报文。点击"停止	"可以截取报文,点	击"下载"可下载已蔽	取的报文。	© ,	动 占 下朝	ž

图 10.4.3 Tcpdump 工具

10.4.4 信息故障收集

WEBUI: 主界面 -> 系统配置 -> 诊断工具-> 信息故障收集

进入信息故障收集页面,点击"收集日志信息",可进行 bld、as_bin 的日志信息收集。 点击"一键清理日志",可清除页面当前数据显示及后台服务器上存储的日志文件。

≣	⊙ 资产管理 ○ 脆弱性检测	☑ 脆弱性模板	◎ 敏感探測	◎ 合规检查	☑ 报告中心	③ 系统配置	
■ 系统状态	◎系統配置 / ◎诊断工具 / ¥信息	汝障收集					
⊢ 报告输出配置	信息故障收集						
↑ 出境填报	收集信息日志 一鍵清理日志	Ā					
○ 诊断工具 ^	log_20240607095705	下载日志					
端口探測工具							
✓ ping工具							
Icpdump工具							
X 信息故障收集							

10.4.4 信息故障收集



十一. Sysadmin 系统配置

Sysadmin 账户登录访问系统配置页面。

11.1 系统状态

系统状态页面,展示设备信息、运行状态、CPU/内存/交换分区使用率、版本号等信息。

🔊 数据安全检查	查工具箱系统 系统和									
a	0 Rickey / 1 Ricks									
₩ 新统权态	图 设备信息									
■ 潮注Biconse	デ部型母 Supermicro	设备外列型号 0123456789	I秘作:张纯 CentOS Linux7.9.2009	CPU 12 検	P979 62.65 G8	交接分区 31.44 G8	बंग तोत 3.42 TB	進行时任 113 天, 05:00:42	版丰可 v6.0.2.2	
回 IP配置管理	回 运行状态					換分区使用率				
© AEGHAR E AF-FORMA ⊗ −HEAN	C ¹ <u>B</u> RE 9.21% 50% 2000 13% 12.55% 2000 2.55% <u>2.55%</u> <u>2.55%</u> 2.55%									
	20000 0 60 5			-0	- LORE -O TORE				05	

图 11.1 系统状态

11.2 漏扫 license

漏扫 license: 可进行漏扫功能的 license 授权操作。

🔊 数据安全检查	查工具箱系统 系统配置			
Ξ	◎系統配置 / 国漏扫license			
■ 系统状态	[] 派初/合直			1 147374
回 漏扫license				
∠ 网络属性	硬件序列号	-	许可证樂型	未變权
团 IP配置管理				
⊙ 漏扫升级				
一 资产识别指纹				
⊗ 一键清除				

图 11.2-1 漏扫 license

操作: 在漏扫 license 页面,点击【上传文件】,选择对应的.dat 文件进行上传,授权 后的页面如图所示。





🔊 数据安全检查:	工具箱系统 条统配置					
a	② 系统范围 / 日 開始icense					
₩ 系统状态	① 授权信息					乙 上传文件
Implicense	硬件序列号	A53CCBF9A3FC0390F5458FC933687DDF	修可证编型	Ride	注册时间	2024-04-29
	许可证到期时间	2024-07-28	最大印数	无限制	并没系统归属任务数	5
	任务并发行创政	500	最大站师数	无限制	并发WEE目编站将数	2
一 资产识别指纹	第日4日第	开启	井发口令强解数	2	重成的	开展
⊙ —#2388						

图 11.2-2 授权后漏扫 license

11.3 网络属性

网络属性: 网络属性页面可查看网卡相关信息,可进行网络地址、掩码、网关的配置等操作。

操作:选择对应的网卡, PING 控制选择"允许"/"禁止",修改地址与掩码, 网关的 配置信息,点击"保存",可成功进行网卡信息的修改。

🔊 数据安全检查3	工具箱系统 系统面	a)	Q ③2024/05.07 H49425 A 統計開發 ▼ 也 與出
ā	◎ 形成形形 / ∠ 网络潮性		
■ 系统状态	这段状态	314-48F 🎓	
Millicense	MAC地址	8/91 d0 66/5cd1	
∠ Misinte	PINGE286	允许 V	
回 19記書管理	地址与编码	Matt.192.168.0.1/255.255.0.0	
② 漏扫升级	同关		
回 资产积弱捐款			
 一號清除 	网络猿口	dosker0	
	法接状态	Natur 🎓	
	MACRELE	24227:707±03	
	PING控制	対 序. マ	
	地址与编码	172.170.1/255235.00	
	网头		
	网络接口	virbi0-nic	
	连接状态	184# •	
E.	MACRENE	2540022b531	
	PINGE280	20# V	
	地址与编码	mth192.166.01/255.255.0.0	
	50 M		
	PER	B 495	
		SC WAY	

图 11.3 网络属性

11.4 IP 配置管理



IP 配置管理:可以进行 kafka IP 或端口信息的配置,也可以进行探针的 IP、端口、镜像网口的配置。

🔊 数据安全检查:	C具箱系统	系統配置		
a	O RIGHER / B	和教育項		
₩ 系统状态	kafka PB			
回 遍归icense	* kafkalP	127.0.0.1	* kafkalij 19092	
∠ 网络属性				
◎ 漏扫升级	1 1891 1218			
回 资产印刷指数	• IP-38CI	172.20.57.51:18099	• 備像月口 enc3	
 一批消除 		健む原		

图 11.4 IP 配置管理

操作: 在 IP 配置管理页面,输入 kafkaIP、kafka 端口信息,点击"一键配置";输入 探针的 IP:端口、镜像网口信息,点击"一键配置",分别进行系统自身 kafka 和探针的信 息配置,如图所示。

11.5 漏扫升级

漏扫升级:可以进行漏扫功能的规则库在线升级、系统/规则库/补丁 FTP 升级、系统/ 规则库/补丁离线升级操作。

図 の Mindem / Q Mainter	
■ 新秋市 A.开级管理	î
G #23:www.	
程 IP4281878	
(0) 期間時 ProsylUEE先發 通信交流的代表地上與研究服务器地址的升级信	
回 #A+408662 代理服务和同户名	
② 一幅描述 代理想方确定码	
44/9 D359/Ha	
	0 V
由前系统版本 V3.0(6.6.1-81-v90757-20230222)	
曲带计T版本 20231221104599	
监察部署 20240319146600	
79028 0.00%	
	-

图 11.5 漏扫升级

操作:准备相应的在线规则库或离线规则库,在漏扫升级页面配置相关的代理服务器信



息或上传本地的离线升级包,点击"升级",进行漏扫规则库的升级,如图所示。

11.6 资产识别指纹

资产识别指纹:进行边界链路的配置,并在资产扫描的结果中匹配对应的资产识别指纹。

🔿 数据安全检查	查工具箱系统 系统	AACIII														
12	O BARACE / ED BP-FBIN	纹														
■ 系统状态	承建厂商 (1912)	ля			現制名称 (3)	N.A.R.SR			WEB 英語城口	WEAwebPort				४ द्वम ९ का स	1 18	CER
■ 期目icense ∠ 阿洛属性	WEB页面关键字 编辑人	with Exe t			设备分类 请	BRIGH OM		U.	规则失型 1	15月9月21			v			
回 19配置管理	▽ 边界链路配置列表													T Omb	9638	+ 1617
◎ 漏臼升级	- 規則各称 >	承建厂商 :	estestes o	第四列表	第四白名单	5400	WEB Silliuri	WEB (A)BIRD	WEB 英国关键字	设备分类	WEB 英语关键	秋志	清除扫描结果		IRA	
亚 资产积累指数	mysql_53306	绥信数科_53306	2024-05-08 15:	\$3306		1				其他	1.000	正常	清缺所有数据	编辑	-	释止
⊙ —#2358	web_443	研想政府。443	2024-05-08 16:				http://	443	sailing54	ME		正荣	清除所有数据	9993	-	傳止
	socket,443	發信股利_443	2024-05-08 16:					443				<u>IE</u> #	湖政府有限第 世政: 3	5858 < 1	> 10.9	停止 6/页~

图 11.6-1 资产识别指纹

操作:在资产识别指纹页面,点击"新增",如图所示,分别填写端口配置、WEB页面 配置、socket 配置,点击"保存"。

新增边界链路配置				Х
* 承建厂商 领信数科_443	*规则类型 数据库资产	✓ * 类型分组 其他	~	*规则各称 mysq_53306
端口配置 WEB 页面配置 soc	ket配置			
端口组			+ 添加端口组	┃ 端口白名单
端口组	间值		操作	多端口请换行
53306,3306,8899	2		ū	<i>i</i>
			< 1 >	
				取消 保存

图 11.6-2 新增边界链路配置

dcbox 账户登录系统,在资产扫描页面查看配置生效结果。




🔊 数据安	全检查	L具箱系统													
=			Bastaren 🖂 Boastaren	to self-rom		i∰ ⊡#64	0 0 5.0 5.0								
1 资产扫描	^	◎ 田产管理 / I 田产	日月 / 🗋 日月日二												
會 扫描任务		资产类型 资产学	1. 12		v.	厂商名称	使信款科			0	IPHELE IPHELE				Q 111日 C 重要
已 扫描結果			- 20			8514	8514				THERE THERE				
		Contract Lines													
回 资产预览	•	扫描结果											T 🖯	出发现列表 + 能量	
图 其它工具	v	常规列表 印度	21W												
		0.00	Г л	资产类型	iPtEtž	STREE IS	是古新发现	开放端口	命中URL	0440	APIF7IZER	设备分类	是否注册	发现时间	8H
		0.1	· (资告数科_53306	数据库总产	172.20.60.3		E	22,111,5005,8082,80	0.000	53306		#/S	律过去册	2024-05-08 16:10:04	25.311 BHRR
		2	發售数科_53306	数据库资产	172.20.57.28	+**	æ	22,111,53306	-	53306		M/S	未注册	2024-05-08 16:10:19	STATE BOOK
		0.3	昭福政末4_53306	数据库资产	172.20.57.29		10	22.111.5005.8082.80		\$3306	4	MG	未注册	2024-05-08 16:10:19	添加 删除
		4	领信数科_53306	数据率资产	172.20.52.57		2	22.111.2181.5005.80		53306	5	#5	未注册	2024-05-06 16:10:22	sin wat
		0.5	领信数料_53306	数据库资产	172.20.52.166		百	80,111,443,2505,999		53306		第 位	未注册	2024-05-08 16:10:23	3530 BERK
		6	研播取和_53306	数据库图产	172.20.66.31		2	22,111,8081,8088,94		\$3306		黄色	未注册	2024-05-08 16:10:29	添加 删除
		7	资信取料_53306	数据库资产	172.20.54.23		百	111,5005,8082,8088		53306	2	其他	未注册	2024-05-08 16:10:36	san ma
		8	發傷数料_53306	数据库资产	172.20.54.52		百	22,111,5005,53306		\$3306		H /2	未注册	2024-05-08 16:10:36	添加 施助
		9	(时图数94_53306	数据库资产	172.20.53.167		÷	49664.49665.49666		53306	(and)	RS	未注册	2024-05-08 16:15:54	30.10 #102
														共计9版 < 1	> 10 祭/贡∨

图 11.6-3 资产识别指纹生效

11.7 一键清除

一键清除:分模块进行数据清除,并记录清除记录。

数据安全检查工具箱系统 系统政策 0 ○ 2024.05.07 14.2035 ▲ Edentities ● ○ aller								
a	© %ARE / ⊙-1239							
圖 系统状态	一線造設							
Implicense	#9	功能模块	满脸次数	清除状态	预计选择时间	操作		
	1	總明住管理	7	已完成	5分钟	海除 海铁记录		
回 IP配置管理	2	洗量探向	7	Best	569	油除 油除记录		
◎ 漏扫升级	3	敏振祥测	2	已完成	5Et	清钟 清钟记录		
亚 资产识别指纹	4	资产管理	18	已完成	582	MH MHZR		
 —uzate 					忠政: 4	〈 1 〉 10 景/页 √		

图 11.7-1 一键清除

操作:在一键清除页面,选择对应的模块,点击"清除"按钮,在弹出的二次确认框中 点击"确定"。相关模块的数据会被清除。

脆弱性管理:清除脆弱性检测-任务管理、脆弱性资产、脆弱性资产组,脆弱性模板-基 线策略模板,报告中心-脆弱性导出;影响资产管理-资产预览-风险资产管理的数据评分;

流量探测:清除流量探测-新建任务、探测预览,报告中心-流量报告、综合报告内容; 影响资产管理-资产预览-风险资产管理的数据评分;



敏感探测:清除敏感探测-敏感数据发现内容;

资产管理:清除资产扫描-扫描任务、扫描结果、区域配置,资产预览-资产台账、资产 测绘、风险资产管理,敏感探测-数据库资产,报告中心-资产台账、综合报告内容。

点击"清除记录",可查看对应模块的清除记录。

🛞 数据安全检查]							
Ħ	O NAME / Q-42478	法除233			×	P	
M NMUTE	1—經濟政	1 PINGAL PR					
🕒 Millionae		成号	功能模块	油和时间	RB		
Z WART		1	統將性管理	2024-04-29 14:34:18	4分钟 54秒		
B PREES		2	脆弱性管理	2024-04-28 20:55:59	4分钟 310		MAY MAYING
0.81110		3	總時性管理	2024-04-28 18:24:09	3/319 4080		THE REAL
G anna		4	脫聯性管理	2024-04-28 18:18:08	25914 2689		
iii Badiriko		8	脆弱性管理	2024-04-28 17:00:14	3分钟 17秒	100 m c 110 m c	AT AND
S -423.00		6	統與性管理	2024-04-28 11:13:58	4()10 5380	思数: 7	2 11 > 10 美/西平
		7	胞弱性管理	2024-04-24 17:03:25	5(310 SE)		
					总数:7 く 1 > 10条/页 >		
					关闭		

图 11.7-2 清除记录