

洞鉴(X-Ray)安全评估系统 产品使用手册

北京长亭科技有限公司

一、自次	访问
1.1 部署	聲并上传 许可证
1.2 登步	₹2
1.2	.1 用户登录
1.2	.2 未登录时顶部导航栏
1.3 首次	次使用注意事项
1.3	.1 引擎权限分配
二、系统	充界面布局介绍 4
2.1 菜	单导航
2.2 面包	回屑
2.3 正3	之区域
三 功能	
	碑块介绍
3.1 扫	·模块介绍 · · · · · · · · · · · · · · · · · · ·
3.1 扫 3.1	7 苗管理
3.1 扫 3.1 3.1 3.1	7 苗管理
3.1 扫 3.1 3.1 3.1 3.1	福賀理 .7 .1 任务统计 .7 .2 扫描策略 .10 .3 任务列表 .15
3.1 扫 3.1 3.1 3.1 3.1 3.1 3.1	福管理 .7 .1 任务统计 .7 .2 扫描策略 .10 .3 任务列表 .15 .4 扫描设置 .28
3.1 扫 3.1 3.1 3.1 3.1 3.1 3.1 3.1	湖管理 .7 .1 任务统计 .7 .2 扫描策略 .10 .3 任务列表 .15 .4 扫描设置 .28 .5 添加扫描任务 .42
3.1 扫 3.1 3.1 3.1 3.1 3.1 3.1 3.1 3.1 3.1	講管理 .7 .1 任务统计 .7 .2 扫描策略 .10 .3 任务列表 .15 .4 扫描设置 .28 .5 添加扫描任务 .42 .6 配置参数模块 .62
3.1 扫 3.1 3.1 3.1 3.1 3.1 3.1 3.1 3.1 3.1 3.1	講管理 .7 .1 任务统计 .7 .2 扫描策略 .7 .2 扫描策略 .10 .3 任务列表 .15 .4 扫描设置 .28 .5 添加扫描任务 .42 .6 配置参数模块 .62 .7 代理服务器配置方法 .120
3.1 扫 3.1 3.1 3.1 3.1 3.1 3.1 3.1 3.1	講管理 .7 .1 任务统计 .7 .2 扫描策略 .10 .3 任务列表 .10 .3 任务列表 .15 .4 扫描设置 .28 .5 添加扫描任务 .42 .6 配置参数模块 .62 .7 代理服务器配置方法 .120 .8 API 扫描文件获取方式 .124



	3.2.1 基线检查任务列表12	7
	3.2.2 检查任务详情13	1
	3.2.3 添加基线任务14	2
	3.2.4 基线检查配置14	7
3.	3 镜像管理	9
	3.3.1 镜像扫描任务列表14	9
	3.3.2 添加镜像扫描任务150	0
	3.3.3 镜像扫描任务详情15	1
3.	4 资产中心	5
	3.4.1 资产全景	5
	3.4.2 主机资产	9
	3.4.3 Web 站点资产列表 17:	2
	3.4.4 资产组列表	2
	3.4.5 资产属性管理-IP 段管理190	0
	3.4.6 资产属性管理-业务系统管理19	2
	3.4.7 资产属性管理-网络区域管理19	5
	3.4.8 资产属性管理−标签管理190	6
3.	5 漏洞管理	8
	3.5.1 漏洞全景	8
	3.5.2 漏洞列表	0
3.	6 报表中心	0
	3.6.1 报表管理210	0
	3.6.2 生成报表	4



	3.6.3 报表模版	19
3.7	知识库	21
	3.7.1 漏洞库	21
	3.7.2 自定义 POC2	23
	3.7.3 自定义指纹	29
四、系	系统管理介绍 23	31
4.1	系统设置	:31
	4.1.1 基本配置	231
	4.1.2 显示配置	:39
4.2	系统信息	242
	4.2.1 基本信息	:42
	4.2.2 状态监控2	:45
	4.2.3 服务状态	247
4.3	系统服务	247
	4.3.1 引擎升级	247
	4.3.2 漏洞库升级	252
	4.3.3 系统升级	252
	4.3.4 备份还原	253
	4.3.5 引擎网络诊断2	255
	4.3.6 扩展管理平台配置	256
4.4	日志管理	257
	4.4.1 操作日志列表	257
4.5	引擎管理	259



	4.5.1 引擎列表	259
	4.5.2 其他扫描配置	263
五、月	用户管理	267
5.1	系统用户管理	267
	5.1.1 系统用户管理	267
5.2	用户角色设置	270
	5.2.1 用户角色列表	270
5.3	组织单位管理	273
	5.3.1 组织单位树	273
六、イ	个人中心模块 2	279
6.1	个人中心	279
6.1	个人中心	279 279
6.1	个人中心	279 279 280
6.1	个人中心	279 279 280 281
6.1	个人中心	279 279 280 281 282
6.1	个人中心	279 279 280 281 282 282
6.1	个人中心	 279 279 280 281 282 283 290

一、首次访问

部署成功后,首先需要长亭科技签发的官方许可证文件,验证通过后,才可使用 洞鉴安全评估系统。

1.1 部署并上传许可证

部署成功后,访问服务器网址,会出现如下界面:

访问已被限制,	请上传	许可证后重新访问
当前机器码:(二二二二二	-	一個复刻
请复制机器码发给相关	工作人员,)	用以申请该机器的访问许可证
	0	
点击或	将文件拖排	國这里上传

- 复制机器码给相关工作人员,申请绑定机器码的 license;
 - 如果授权的 license 绑定的机器码与当前机器码不符,则无法认证成功,需重新上传。
- 点击或拖拽许可证文件;
- 上传正确的许可证文件后,会显示初始用户名、初始密码、被授权的企业名称和授权使用时间,管理员确认无误后,点击"确认",即可完成许可证的更新,此时许可证内容显示新上传的许可证信息。

注意:这一步注意要复制好密码,点击"确认"后,需要用此密码登录。



加始用户名	admin
7)始密码	
度度权企业名称	or the lot of the lot
夏权使用时间	2019-02-01 - 2019-12-31
最大并发任务数	6
是权机器码	100
曲认以上许可证信	息是否正确

● 此时的初始用户名和初始密码,在许可证信息上传成功后,用于登录系统。

1.2 登录

1.2.1 用户登录

● 输入正确的用户名和密码后进入主页面。

<┅ 洞鉴x-RAY		长亭科技冒険 长亭科技帮助中心
	用户登录	
	R 用户名	
	日期日	
	登录 山口で発明、 現然系令(水田等等日本の市は東本市村は	
	4-48-68791,可如用出品用用品用品品用品用品品以下不用用132 有限公司指关技术支持负责人寻求帮助	
	X-Ray XR-\$10 21.11.001_r10 @ 2021 Chaitin Tech.	

温馨提示:如忘记密码,请联系企业系统管理员或公司相关技术支持负责人寻求帮助。



1.2.2 未登录时顶部导航栏

可导航至长亭科技官网和帮助中心

<₩ 洞\subset x-RAY		长亭科技官開 长亭科技帮助中心
	用户登录	
	R 期户名	
	品 激弱	
	登录	
	如后记图码,调制系企业系统管理员或定员长亭未来科技 有限公司相关技术支持负责人寻求帮助	
	X-Rey XR-S10 21.11.001_r10 @ 2021 Challin Tech.	

1.3 首次使用注意事项

1.3.1 引擎权限分配

新部署的引擎权限默认未配置,需要手动分配成公有或私有的权限

<→洞巖×	RAY								(admin
WUL 作区	¥	2.11.11.11 × 11.11.11.11						编辑引擎	×
· saare R meen R		510758 Proteinan + IRAIRIDS-9						引擎基本信息 引擎56点 109.224 1.1	
* 2.**0			51111 A #	167700	引要权用	**	CPU DERE	11章各称 公共引擎 *11章权服 公共	
E REPO		A A A A A A A A A A A A A A A A A A A		120				H版 NTE-4015000	
o Arter Artice Artice Arter UCRE						, a 4 ₉₀ an 644 to 54	302.003, 47 52 2004 (Diversi Tech -	第11 年 11	an r tait
1.864								以下代理局负荷,用于为被迫 Web 编码扫描任务提供需要的代理服务器估测。	
- Rote								代理協会哲学 500-254.1.1 HTTPS 相互任 ② 点金工程 HTTPS 修正来 基子日志的特征原生的 Systeg 服务指定度 NTC Assess 局景語 高工 ASS NT I D-01/08/15 Mark 10/07/09/06/14 (4)/4 00/09/09/14	na marca na con na c

二、系统界面布局介绍

2.1 菜单导航

洞鉴(X-Ray)安全评估系统菜单栏从全局仪表盘、扫描管理、基线管理、镜像管理、 资产中心、漏洞管理、报表中心、知识库、系统管理、用户管理进行分类展示。

2) 全税以表型 2) 日源管理 ~ 3) 日源管理 ~ 4) 差 然管理 ~ 4) 登 定 深同增长来: 0.00% 第名公上占比: 32.0% 2) 目前指端回中数: 0 一 2) 服用能 - 自定 X POC - 自定 X POC - 自定 X POC - 6 - 6 - 6 - 7 - 6 - 6 - 6 - 6 - 7 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - <th>清空的 已修复漏洞总数 42</th> <th>服存 跳转到</th>	清空的 已修复漏洞总数 42	服存 跳转到
日本程程 ・ ・ ・	已修复漏洞总数 42	
	42	
 第产中心 → 第定数 → 行分配漏洞增长来:0.0% 第危及以上占は:32.0% 当日新増弱口令数:0 ご 伊登重演測増长来:0.00% 注 日新増弱口令数:0 ご 伊登重演測増长来:0.00% 第た及数上占は:32.0% 第合数 量統计 第方运行情况 第方 通行及 塗 367 売 気 3 市 行活 3 市 利 162 主 机灵产数 186 第181 未知 1 未知 1 未知 1 	74	
変変変更 特分配温润增长率:0.0% 液危及以上点比:32.0% 当日斯塘碧口今数:0 已修复温润增长率:0.0% 損食中心 第 第 第 第 第 第 第 第 第 第 第 第 第 第 第 第 第 第 1 第 第 第 1 <th1< th=""> <th1< th=""> 1</th1<></th1<>		
損表中心. 次 资产运行情况 资产风险等级分布 知识库 ・ 第广总数 367 第广总数 186 追究文 POC ・ ・ 日定文 作 5 活 3 182 181 自定文和区 ・	平均漏洞修复时间 4	4周3天
知识年 ^ 変形意数 367 変形意数 367 変形意数 186 自定文 POC ・存活 182 主肌灵产数 186 ・不存活 3 Web 资产数 181 ・未知 1 未知风险资产 1		
第3時 ・存活 182 主机员产数 186 自定义 POC ・不存活 3 Web 型产数 181 自定义組成 ・未知 1 未知风险资产 1		1 7.22
自定义 POC ・ 不存活 3 Web 型产数 181 自定义E版2 ・ 未知 1 未知风险资产 1	 高危资产 中危资产 	97
自定义指纹 • 未知 1 未知风险资产 1	• 低危资产	9
	• 安全资产	256
系統實理 · 不存活流产数 0.8%	 未知资产 	1
用户管理 イ		
风险资产组织单位 Top 5 业务系统漏洞排名 Top 5		
排名 组织单位 资产总数 漏洞总数 影响 排名 业务系统 资产总数	数 漏洞总数	影响

- 全局仪表盘:从全局提供一些关注度高的信息统计视图,如漏洞、资产等。
- 扫描管理:存放扫描相关的各项操作和数据展示内容:
 - 任务统计:包括任务概览、结果统计
 - 扫描策略
 - 任务列表
 - 扫描设置
 - ◆ 字典管理
 - ◆ 端口组管理
 - ◆ 全局白名单配置
 - ◆ 盲打平台监听配置
- 基线管理:包含基线检查相关的数据和操作
 - 基线检查任务列表:包含在线检查列表、离线检查列表、离线本地列表
 - 基线检查配置
- 镜像管理:包含镜像检查相关的数据和操作
 - 镜像扫描任务列表
- 资产中心:此模块主要用于企业的资产进行管理,系统将企业的资产数据进行综合统计计算并可视化,方便直观的展示给用户,并支持对已知资产与未知资产进行集



中管理,包括对资产的查询、筛选、添加、删除、快速扫描等操作。企业可对资产 进行分组和指派责任人、管理员。

- 资产全景
- 资产列表
 - ◆ 主机资产列表
 - ◆ Web 站点资产列表
 - ◆ 资产组列表
- 资产属性管理
 - ◆ IP 段管理
 - ◆ 业务系统管理
 - ◆ 网络区域管理
 - ◆ 标签管理
- 漏洞管理:方便用户对系统所有漏洞、有风险的资产进行管理
 - 漏洞全景
 - 漏洞列表
- 报表中心:对已生成的不同类型报告的管理
 - 报表管理
 - 报表模板:包括扫描任务报表、基线检查报表、资产报表、漏洞报表
- 知识库
 - 漏洞库
 - 自定义 POC
 - 自定义指纹
- 系统管理
 - 系统设置:包含基本配置、显示配置、网络配置
 - 系统信息:包含基本信息、状态监控、服务状态
 - 系统服务:包括引擎升级、漏洞库升级、备份还原、引擎网络诊断、网络诊断 工具
 - 日志管理
 - 引擎管理:包括引擎列表、其他扫描配置
- 用户管理
 - 系统用户管理
 - 用户角色设置
 - 组织单位管理
- 个人中心
 - 个人中心:包含个人基本信息,修改登录密码
 - Open API
 - 退出



2.2 面包屑

↔洞鉴×	-RAY						admin
认工作区	. v [旧管理 / 任务统计					
全局仪表盘		任务概算 结果统计					
扫描管理	~						
任务就计		不同扫描策略的任务数量分布				最大并行任务数统计	
1316 16 18			• # •	基	• 报		
			• ig •	特	• 被		N 0
任务列表			● 被 ●	被	• w	BI@##74.839	
扫描设置	~		• 披 •	主	● 报	B	
M 54 99 19			• 逻 •	被	= kk		
			• 5 •	e	 希看 		
^{我严中心}	~						
國內管理	~						
服表中心	~	新发现的漏洞数量趋势分析					
		60000				◇ 全部 ◆ 严重 ◆ 再	馬危 🔶 中危 🕳 低危
知识库	~	45000					
系统管理	~	30000					
用户管理	~			0			
		15000		1	1		

 面包屑主要作为辅助导航,帮助用户方便定位当前所处的位置,快速进入到上一级 或更上一级的页面;

2.3 正文区域

左侧导航栏右方的区域展示正文的详细内容。用户可在此进行查看、扫描和管理等 各种操作。详情可以查阅下文三、四、五章中,对各功能模块的详细介绍。

三、功能模块介绍

主要功能有:扫描管理、基线管理、镜像管理、资产中心、漏洞管理、报表中心和 知识库。

3.1 扫描管理

3.1.1 任务统计

在左侧导航栏中,选择"扫描管理-任务统计",进入扫描任务列表界面。

<->洞鉴x-RAY 默认工作区 3項管理 / 任务统计 ◎ 全部位表盘 任务概定 结果统计 Beret 查看维度: 2021-12-17-2021-12-24默认工作区 这种数据聚合组成 任务机计 1112/0185 风险目标数 / 扫描目标数 漏洞总数 待修复漏洞数 11-16-21-20 216/404 39084 39081 白喉没葉 1532 1182 10889 25501 1529 1182 18868 25501 ABREE 5 8/P (P (A) 统计扫描记录 -* 30122 漏洞等级 编码权量 重用名称 **建筑影响位置** 漏洞状态 日 我表中心 110 99% Web 基础认证我口令调制 •1 •0 •0 •0 •0 •0 + CI 102/4 89% Web 表单發口令萊莉 •0 •0 **CB** • 3 .0 O SATU 100 89% Web 基础认证或口令课题 •0 •0 0 A 用户管理 . 0 78 Web 表单联口变漏洞 99% . 0 **FB** 99% Web MRKATERIT-9-38190 . 0 -Web 表单弱口变黑洞 99% •0 •0 •0 . 0 78 99% Web 基础认证成口令演调 •1 •0 •0 •0 •0 •0 -•3 •0 •0 •0 •0 •0 4 99% Web 表单级口令運用

任务统计页面展示系统中的任务概览和结果统计。



3.1.1.1 任务概览

不同扫描策略的任务数量分布				最大并行任务数统计
	• 基	• 基	• 被	
	• 域	• 特	• 被	
	• 被…	◎ 被	• w	
	• 被	• 主	● 被	利乐并行任务数 8
	• 逻	• 被	◎ kk	
	• 5	• e	 看看 	

- 不同扫描策略的任务数量分布:
 - 展示不同扫描策略的任务数量, 鼠标悬浮在饼图上方可以看到具体的任务数。
- 最大并行任务数统计:
 - 展示系统当前正在并行的任务数(正在运行的任务总数),以及剩余并行任务数(还能够同时运行的任务数量);
 - 最大任务并行数由 license 配置决定。

1000										~ 21	◎ ◆ 严重 ◆ 高哉 ◆ 中危 ◆ (
1500											
5500											
0, 12月23日 12月24日	12月26日	12月26日	12月27日	12月28日	12月29日	12月30日	12月31日	01月01日	01月02日	01月03日	01月04日 01月06日 01
現的资产数量趋势分析											域名 主机 服务 (
160											\frown
120											
80											
40											

- 新发现的漏洞数量趋势分析:
 - 展示系统最近 15 天内, 新发现的漏洞数量趋势;
 - 鼠标悬浮在图形上方,可以看到当天新发现的各个风险等级的漏洞数量。
- 新发现的资产数量趋势分析:
 - 展示系统最近 15 天内,新发现的资产数量趋势;
 - 鼠标悬浮在图形上方,可以看到当天新发现的资产数量;
 - 点击图形右上角的按钮,可以切换展示不同资产类型的趋势分析。



存在漏洞的任务			
排名	任务名称	漏洞数量	扫描时间
1	web測试	492 312 5427 5256	2021-12-15 15:40:20
2	浏览器爬虫test	403 331 6350 6157	2021-12-21 15;28:32
3	https://192.168.50.13:8443/benchmark	148 186 0 137	2021-12-20 12:33:02
4	http://10.3.0.4:8070/	43 💽 💽 🖪	2021-12-20 19:38:34
5	主机测试	42 196 428 2023	2021-12-16 10:15:04
6	nnn	37 443 360 1467	2021-12-01 11:51:37
7	http://10.3.0.4:8070/	22 🖸 🚺 🖬	2021-12-20 18:20:27
8	http://10.3.0.5	20 11 20 22	2021-12-20 18:20:48
9	. t	15 10 20 103	2021-11-29 15:18:42
10	đ	15 [4 22 [100	2021-12-06 11:41:09

- 存在漏洞的任务:
 - 展示所有存在漏洞的任务,方便用户直观地找到最需要处理与排查的任务;
 - 任务的排名由任务发现漏洞的风险程度决定:严重漏洞越多,排名越高;严重 漏洞相同的任务,高危漏洞越多排名越高;以此类推。

3.1.1.2 结果统计

- 选择聚合维度操作:
 - 用户可以选择展示的维度,其中包含扫描任务、扫描时间、创建用户和组织单位;

扫描任务	×			~ 劒間
扫描时间	× .	开始日期	~ 结束日期	
创建用户	×.			E R
组织单位	×]			
+ 添加条件				

● 扫描漏洞信息:



风险目标数 / 扫描目标数	灟润总数	待修复漏洞数
<mark>424</mark> /1555	56594	56590
	1658 1585 22067 31284	1654 1585 22067 31284

● 统计扫描记录:

统计扫描记录	漏洞列表			
排名		任务名称	濕润数量	扫描时间
1		kxueV	a 🖬 💷 🚥	2021-12-23 14:38:50
2		浏览器爬虫test	403 331 4850 6157	2021-12-21 15:28:35
3		http://10.3.0.4;8070/	43 💽 🛄 🖪	2021-12-20 19:38:36
4		dvwa	5 85 66 (10)	2021-12-20 18:28:19
5		http://10.3.0.5	20 11 20 02	2021-12-20 18:20:49
E.		浏览器爬虫test	418 324 8811 6107	2021-12-20 18:20:49
U.		http://10.3.0.4:8070/	21 0 0	2021-12-20 18:20:28
r.		dvwa	2 20 00 000	2021-12-20 18:15:58
1		http://10.3.0.4:8070/	21 🔟 🛄 🖪	2021-12-20 18:15:48
0		http://10.3.0.4:8070/	o 🖬 🛤 😆	2021-12-20 18:14:03
				< 1 2 3 4 5 6 7 > 跳至

漏洞列表信息:

	漏洞等级	漏洞权重	漏洞名积	漏洞影响位置	漏洞》	恷				
		99%	Web 基础认证弱口令漏洞	1	• 1	• 0	• 0	• 0	• 0	• 0
	-	99%	Web 表单弱口令漏洞	3	• 3	• 0	• 0	• 0	• 0	• 0
Ð	-	99%	Jboss 管理后台弱口令漏洞	1	• 1	• 0	• 0	• 0	•0	• 0
ł.	-	99%	XML 实体宣注入漏洞	5	• 5	• 0	• 0	• 0	• 0	• 0
ţ.	70	99%	XML 实体回显注入漏洞	З	• 3	• 0	• 0	• 0	• 0	• 0
51	78	99%	通用命令注入漏洞	4	• 4	• 0	• 0	• 0	• 0	• 0
ł.	/ =	99%	SQL 盲注入漏洞	60	• 60	• 0	• 0	• 0	• 0	• 0
		99%	PHP 代码注入漏洞	4	• 4	• 0	• 0	• 0	• 0	• 0
į.		99%	任意文件上传漏洞	7	• 7	• 0	• 0	• 0	• 0	• 0
		99%	Web 基础认证弱口令逼润	3	• 3	• 0	. 0	• 0	.0	• 0

3.1.2 扫描策略

在导航栏中,选择"扫描管理--扫描策略",进入列表界面。



(→ 洞鉴x-	-RAY							admin
心工作区	Y	白奇世世(白榆葉略						
) 28088 118888	~	日間繁時快速防造 () 在急策略 (用限制用中位 数以工作区 ×)	+ 激加筛选条件					
任务统计		● 已选择 0 个扫描简略					+	anti ini ma
118.848		□ ~ 目描策略名称	扫描策略描述		创建单位	扫描策略类型	日搭策略添加时间	10.15
任务对表		基础 Web 派羽扫描	针对 Web 站点进行全面的资产发现和漏洞扫描		0940	系统内置	2021-11-29 14:33:57	日期
白曜设置		基础服务混购日报	针对主机进行全面的资产发现和漏洞扫描		(; ;)	系统内置	2021-11-29 14:33:57	EM
基线管理	×	被助 Web 目標 (代理)	善于 nttp. 代理,对 Web 站点进行被动漏洞扫描		0.00	系统内置	2021-11-29 14:33:57	目期
京が中心 高市管理	2	1 城名资产发现	针对城客进行全面的资产发现		(4)	系统内置	2021-11-29 14:33:57	FIM.
报表中心	•	- 総助 Web 扫描(日志)	基于日志,对 Web 站直进行被动调调扫描			系统内置	2021-11-29 14:33:57	白蜡
NO FOR	0		基于情像流量,对 HTTP 流量进行被动收集和演员扫描		1027	系统内置	2021-11-29 14:33:57	扫描
系统管理	2	□ 被动服务扫描 (镜像)	基于镇像流量搜集目标并扫描		1553	系统内室	2021-11-29 14:33:57	HM
用户管理	~	主机防产监控	对企业资产进行定期巡检、监控企业资产的变更情况		0.00	系統内置	2021-11-29 14:33:57	日編
		被动资产发现(镇像)	基于镇像流量对资产进行贸易发现		1002	系統内置	2021-11-29 14:33:57	白腹
		前定服务扫描	针对特定服务进行漏洞扫描		194 1	系统内置	2021-11-29 14:33:57	日旗
						< 1 2	> 10条/页 /]	<u>未至</u>
				N. Day, MD. 040 (91 +14 JULY -105 II) (2010) (2010) (2010) (2010)				

扫描策略主要用于在创建扫描任务时,提供扫描规则模板,实现一键式便捷快速扫描。扫描策略总体分为以下两类:

- 系统内置扫描策略:
 - 主机扫描:
 - ◆ 主动扫描:基础服务漏洞扫描
 - ◆ 被动扫描: 被动服务扫描(镜像)
 - Web 扫描:
 - ◆ Web 主动扫描:基础 Web 漏洞扫描、逻辑漏洞扫描
 - ◆ Web 被动扫描: 被动 Web 扫描(代理)、被动 Web 扫描(日志)、被

动 Web 扫描(镜像)、 被动 Web 扫描(KafKa)

- API 扫描:
 - ◆ 被动 API 扫描 (OpenAPI)
- 资产发现与监控
 - ◆ 域名资产发现
 - ◆ 被动资产发现(镜像)
 - ◆ 主机资产监控
- 自定义扫描策略
 - ◆ 由用户基于系统内置扫描策略,自行配置具体参数而建立



3.1.2.1 内容展示

8.4	扫提策略名称	扫描策略描述	创建单位	扫描策略类型	扫描策略添加时间	操作
	基础 Web 漏洞扫描	针对 Web 站点进行全面的图产发现和漏洞扫描		系统内置	2021-11-29 14:33:57	日描
	基础服务编词扫描	针对主机进行全面的资产发现和漏洞扫描		系统内置	2021-11-29 14:33:57	扫描
	被动 Web 扫描(代理)	基于 http 代理,对 Web 脑点进行被动漏洞扫描	-	系统内置	2021-11-29 14:33:57	扫描
	域名资产发现	针对域名进行全面的资产发现	100	系统内置	2021-11-29 14:33:57	扫描
	被动 Web 扫描(日志)	基于日志,对 Web 站点进行被动属洞扫描		系统内置	2021-11-29 14:33:57	扫描
	被动 Web 扫描(镜像)	基于镜像流量,对 HTTP 流量进行被动攻集和漏洞扫描		系统内置	2021-11-29 14:33:57	扫描
	被动服务扫描(镜像)	基于硯像流量投集目标并扫描		系统内置	2021-11-29 14:33:57	扫描
	主机资产监控	对企业资产进行定期连检,监控企业资产的安更情况	12	系统内置	2021-11-29 14:33:57	扫描
	被动资产发现(镀像)	基于领像流量对资产进行探测发现		系统内置	2021-11-29 14:33:57	扫描

当使用自定义扫描策略进行扫描任务时,可开启扫描策略自动同步按钮,开关打开 后,无法修改策略参数。

任务信息		
扫描策略名称	beshishanchu	
使用自定义策略为模拟 步变更:开关打开后, 争数 扫描策略自动同步 ③	的任务支持同 无法修改策略	
* 扫描任务名称 ③		
备注		
* 扫描目标	手动输入 上传目标文件 指定资产组	
	扫描目标構式: 1.1.1.1 1.1.1/24 1.1.1.1/25 1.1.2.3* 1.1.2.3* 2001:0dx8:364d:0015:0000.0000:1a2f:1a2b	
	(又會	建任务 创建并立即扫描任务

3.1.2.2 快速扫描

● 每个扫描策略后均有"扫描"的操作,可以点击快速创建扫描任务,作为启动任务

的快速入口,任务参数配置见 3.1.5 添加扫描任务。



扫描策略名称	扫描策略描述	創建单位	扫描策略类型	扫描策略添加时间	操作
基础 Web 漏洞扫描	针对 Web 站点进行全面的资产发现和漏洞扫描		系统内置	2021-11-29 14:33:57	扫描
基础服务漏调扫描	针对主机进行全面的资产发现和漏洞扫描		系统内置	2021-11-29 14:33:57	扫描
被动 Web 扫描(代理)	基于 http 代理,对 Web 站点进行被动漏洞扫描		系统内置	2021-11-29 14:33:57	扫描
域名资产发现	针对域名进行全面的资产发现		系统内置	2021-11-29 14:33:57	扫描
被动 Web 扫描(日志)	基于日志,对 Web 站点进行被动漏洞扫描	(2)	系统内置	2021-11-29 14:33:57	扫描
被动 Web 扫描《镜像》	基于镜像流量,对 HTTP 流量进行被动收集和源润扫描		系统内置	2021-11-29 14:33:57	扫描
被动服务扫描 (镜像)	基于镇像流量搜集目标并扫描		系统内置	2021-11-29 14:33:57	扫描
主机资产监控	对企业资产进行定期返检。监控企业资产的变更情况		系统内置	2021-11-29 14:33:57	扫描
被动资产发现(镜像)	基于镜像这量对资产进行保测发现		系统内置	2021-11-29 14:33:57	扫描
特定服务扫描	针对特定服务进行调调扫描		系统内置	2021-11-29 14:33:57	扫描

3.1.2.3 筛选操作

通用条件筛选

在此页面,可对扫描策略进行筛选操作,可根据扫描策略名称、扫描策略描述、扫描策略类型、扫描策略添加时间,自由添加一个或多个条件进行筛选,筛选条件之间为并集关系。

日提策略快速转达 🗌 回急 (市風組织学位 默以工作区 ×)	策略 + 源加降速条件				
 已选择 0 个扫描策略 	MITTA: 20, 4+45(21-24)200 mb			+	洋加扫描简略
□ ✓ 扫描策略名称	扫描策略措述	创建单位	扫描策略类型	扫描策略添加时间	操作
🗍 基础 Web 漏洞扫描	针对 Web 站点进行全面的资产发现和漏泥扫描	1.81	系统内置	2021-11-29 14:33:57	扫描

添加筛选条件	×
扫描策略名称 > 请输入要筛选的内容 + 添加筛选条件	
	取消保存

例如: 应急策略筛选

应急策略主要用于新爆发漏洞的检测。对于漏洞爆出后,发布的应急扫描策略一旦 在产品上更新,再次直接筛选出来可对应急策略进行编辑,或直接去创建扫描任务。



通知的单位 默认工作区 ×	目前消除失到 应急策略 ×) +	· 漆加筛选条件				
已选择 0 个扫描策略	臺縣送中的目擔策略				1	+ xstolelia
日描策略名称	扫描策略描述			创建单位	扫描策略类型 扫描策略添加时间	操作
			验无数据			

3.1.2.4 删除操作

支持选择一个或多个自定义扫描策略,对已选的自定义扫描策略进行删除操作。系统内置扫描策略不可被删除,用户只能删除自定义扫描策略。

<・>洞鉴 _{x-RAY}							admin
默认工作区 🗸 🗸	目標管理 / 扫描策略						
◎ 全局仪表盘	扫描策略快速筛选	□ 应急策略					
8 扫描管理 *	所属组织单位 默认工作	车区 ×) + 添加筛选条件					
任务统计	 已选择1个扫描 	策略				批量操作 > +	添加扫描策略
日接触時	☑ > 扫描策略名	称 扫描策略描述	创建单位	扫描策略类型	扫描策略模版	删除	操作
任务列表	i 被动 Web 打	3描(流量) 基于软件的方式采集工具	具所在	系统内置	2	2023-06-23 17:27:28	扫描
扫描设置 ^	Matest自知	E义策略 无所谓啦	默认工作区	自定义	基础服务漏洞扫描	2023-06-27 16:04:36	编辑 扫描
字典管理							
端口相管理					< 1	2 > 10 条/页∨	就至 页
A CONTRACTOR OF							

3.1.2.5 添加扫描策略

由扫描策略列表页的"+添加扫描策略"进入,可进行自定义扫描策略的添加操

作, 具体步骤如下:

- 点击"+添加扫描策略",跳转到添加扫描策略界面;
- 配置扫描策略基本信息:
 - 输入扫描策略名称、描述;
 - 选择策略创建单位,默认为当前所在默认工作区;
 - 上传扫描策略图标,默认为洞鉴图标;



④ 基本信息		2) 选择基础策略	③ 扫描策略参数
	* 扫描策略名称		
	* 扫描策略描述		*
	* 策略创建单位 ①	默认工作区	×
	扫描策略图标	+ 上传	
			F- 9

● 点击"下一步",点击选择扫描策略依据的基础策略:

■ 依据的基础策略可以是系统内置扫描策略,也可以是自定义的扫描策略;

5118	0 :	br# 浙 山 第 略	(i) 1000
● 新聞 A A A A A A A A A A A A A A A A A A		(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	维名资产发现 任时经书进行主题的资产发现
(日本) 왕왕 Web 扫描(日本) 공구日本, 저 Web 브레레카	日日 NG20 Web F318 (現像) 品子母像素単、NI HTTP 洗量	第10年期間、10年期間、10月間、10月間、10月間、10月間、10月間、10月間、10月間、10月	主机用产量的 林生亚用产用行用制度的。 篇
● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	· 特定服务扫描 计可可定服务进行重用扫描	通日的第三人 第1日第三人称单数	(1) () () () () () () () () () () () () ()
Apache Fink-jobmanager/B Apache Fink jobmanager/B			

- 点击"下一步",配置扫描策略具体参数
 - 可自行对每一项参数进行设置;
 - 上一步选择不同的基础策略,所需要配置的参数会有所不同,参数配置的详情 可以参考 3.1.5 添加扫描任务;
 - 扫描策略默认参数配置完成后,点击"完成",创建扫描策略成功,可以在扫描 策略列表页查看。

3.1.3 任务列表

在左侧导航栏中,选择"扫描管理-任务列表",进入任务列表界面,展示系统创建的所有扫描任务信息:



工作区	VE	回音管理 / 任务列表						
全形仪表面		- SHING BUIGS	+ 湖加锦选条件					
10.00	*	 已选择 0 个扫描任务 	REPORTED BOTT	PIEM PIEM				+ attentiv
任务 <i>统计</i> 印服策略		- 扫描任务名称	扫描策略	创建用户	所屬組织单位	扫描计划	日播状态	an
193 1 8		CRTSN	基础 Web 漏洞扫描	admin	默认工作区	Æ	② 扫描结束 (成功)	\triangleright
日編设置	*	kaueV	基础 Web 漏洞扫描	admin	默认工作区	无	② 扫描結束 (成功)	
活管理	×	test	主机资产温程	admin	默认工作区	ž	② 扫描结束 (成功)	
(产中心 (研究者	×	nLWaX	基础 Web 漫词扫描	admin	默认工作区	×	② 扫描结束 (成功)	(\mathbf{b})
8中心	×	Mai.	基础 Web 週间扫描	admin	默认工作区	Æ	② 扫描结束 (成功)	
ene enere	č	KgDmO	基础 Web 週詞目編	admin	默认工作区	充	 EI酸胡米 (成功) 	(\triangleright)
^管理	×	yzsit	基础 Web 满词目缀	admin	默认工作区	Æ	(認知,來訪前日 〇)	$\langle \widehat{ \mathbf{D}} \rangle$
		iQdQy	基础 Web 测测扫描	admin	就认工作医	Æ	扫描结束 (失敗)	(\triangleright)
		DPOH	基础 Web 测测扫描	admin	默认工作区	Æ	② 扫描框束 (成功)	
		rzOUu	基础 Web 建羽扫描	admin	W 以工作区	无	② 扫描結束 成功	(Þ)

3.1.3.1 表头配置

在列表尾部可以对列表表头进行配置操作,可以自定义展示更多信息

are a particulary						批論的	TF V	2007/03=191	812.55
扫描任务名称	风险等级	扫描策略	创建用户	所属组织单位	扫描状态	最近扫描时	间	操作	10
123	无风险	基础 Web 漏洞扫描	admin	默认工作区	⊘ 扫描结束 (成功)	2022-11-] 全选 [] 1388-05-3		11
asdf	(2)	基础 Web 漏洞扫描	admin	默认工作区	21	÷	 (2) 月前等级 (2) 月前等级 (3) 月前等级 		
asdf	273	基础 Web 漏洞扫描	admin	默认工作区	~	<i>s</i>	☑ 包建用户		
为了漏洞	意风脸	基础服务漏洞扫描	admin	默认工作区	⊘ 扫描结束 (成功)	2022-11-	✓ 所属组织单	位	
http://10.3.0.5:9000	高风脸	基础 Web 漏洞扫描	admin	默认工作区	② 扫描结束 (成功)	2022-11-	 ✓ 扫描状态 ○ 创建时间 		
admin10.3.0.5	**	基础服务漏洞扫描	admin	默认工作区	⊘ 扫描结束 (手动结束)	2022-11-	 ✓ 最近扫描时 □ 扫描时长 	间	
10.9.33.192:65412	*30	基础 Web 漏洞扫描	admin	默认工作区	② 扫描结束 (手动结束)	2022-11-	IQ 7	j 📔	呆存
有和没有不一样	未知	基础服务漏洞扫描	admin	默认工作区	② 扫描结束 (手动结束)	2022-11-1	0 16:02:07	(\triangleright)	

3.1.3.2 筛选操作

在列表页可对任务进行筛选操作,可根据扫描任务名称、扫描策略、扫描计划、创建时间、下次执行时间、扫描状态、创建用户、所属组织单位,自由添加一个或多个条件进行筛选。



扫描任务名称	~	请输入要筛选的内容	
上 法hn 随进来从			

● 若想删除筛选条件,点击已添加条件右侧的"X"按钮,即可删除条件。

Sugar 0 Trainettas	新建造中的扫描任务	验停任务 停止任务				+ 液加当播任
▽ 扫描任务名称	扫描策略	创建用户	所属组织单位	扫描计划	扫描状态	操作
			智无数据			

3.1.3.3 批量操作



删除操作

● 在列表页一旦执行删除操作,所有已选任务的记录均将被删除。

启动任务、暂停任务、停止任务

在列表页可以对任务直接进行操作,可进行的操作包括立即扫描与停止扫描。

- 启动任务:对非正在扫描的任务,可以进行立即扫描的操作,具体步骤为:
 - 点击任务右侧操作栏的"启动"按钮,即可进行立即扫描的操作。任务扫描状态变为等待扫描或者正在扫描,操作图标显示"暂停"和"停止"按钮;
 - 进行立即扫描的操作后,任务将按照最新保存的参数配置进行扫描。
 - 注意:系统正在扫描的任务达到了最大并发任务数时,新启动的任务将进入等 待扫描状态。



- 暂停任务:对正在扫描的任务,可以进行暂停扫描的操作,具体步骤为:
 - 点击任务右侧操作栏的"暂停"按钮,即可进行暂停扫描的操作。任务扫描状态变为已暂停,操作图标显示"启动"和"停止"按钮;
 - 进行暂停扫描的操作后,任务自动保存当前扫描的进度,以便于后续进行断点 续扫。
 - 注意:暂停任务的断点记忆存储没有限制,但需要消耗大量资源。如果是手动 暂停的任务,扫描状态显示为"暂停扫描(手动)",如果是系统因时间设置等 原因暂停任务,扫描状态显示为"暂停扫描(系统)"。其中手动操作的优先级 高于系统操作。手动暂停后,任务将不会自动启动扫描
- 停止任务:对正在扫描或等待扫描的任务,可以进行停止扫描的操作,具体步骤为:
 - 点击任务右侧操作栏的正方形按钮,显示确认操作的提示弹窗;
 - 点击弹窗中的"确定",即可完成停止扫描的操作。任务扫描状态变为扫描结束, 操作图标显示"启动"按钮。

扫描任务名称	扫描策略	创建用户	所属组织单位	扫描计划	扫描状态	操作
tvisi	基础 Web 漏洞扫描	admin	默认工作区	无	、 正在扫描	•
KotucV	基础 Web 漏洞扫描	admin	默认工作区	无	暂停扫描	
KgDmO	基础 Web 漏洞扫描	admin	默认工作区	£	② 扫描结束 (成功)	\triangleright

暂停计划、启用计划

在列表页可以对任务直接进行操作,可进行对选中任务的定时扫描计划的批量暂停 和恢复。

暂停计划:对任务进行定时扫描计划的暂停,扫描计划暂停后,从下次周期性扫描的时间开始,该任务的计划将不会被执行,处于扫描计划处于已禁用状态

跳过扫描计划

◎ 每周三的 17:59:00、周一的 18:03:00、周三的 18:05:00 定时扫描 下次扫描时间为 - (已禁用)

● 启用计划:对任务进行定时计划的再次启用,启用后,扫描计划回复正常

生成报表

在列表页可以批量选择任务进行生成报表操作。



3.1.3.4 添加扫描任务

点击"添加扫描任务"按钮,选择要使用的扫描策略模板,然后进行任务参数配合, 详情见 <u>3.1.5 添加扫描任务</u>。

3.1.3.5 查看任务详情操作

点击列表上的扫描任务,即打开扫描任务详情页,可看到该任务的详细信息。

くシ洞鉴。	K-RAY						admin
默认工作区	×	日1011年世 / 任务形制 / test666					
◎ 全用反表盘		test666		结果对比	扫描历史 * 生成报表	\$101218(1.9)	立(013) 6
						10.00	任务扫描计划
任务统计		haha					
扫描繁新		任務統計 漏洞 (0) 維名 (0) 主机 (0) 服务 (0) Web 詰点 (0)					
任务列表		A CARACTER CONTRACT CARACTER AND A CARACTER A					
扫描设置		扫描日本	下载日志 查看更多	任务基本信息			
d Bittin	1			任务状态	扫描结束 (失敗)		
© ₫₽₽0	*	[11:40:00] (状态変更) 任务 [tast666] : 等特時期 → 田道結束 (失敗), 原語: 発電 [11:40:00] (扫描結束)		白翅開晒	基础服务调用扫描		
合 漏洞装理	v			启动时间	*		
信 服務中心	6			扫描时代	0:00:00		
🖾 आसाव	*			日相目物	0 2078		
S KREE				存活主机数量	0		
A 8298	~			天明应主机数量	o.		
10. 10.				已归报主机数量	0		
		運用軟量		推定扫描时段	-		
				指定禁臼时险	12:40 - 14:40		
		③ 猶无說謝					

在任务详情页可以查看任务执行后的扫描结果,还可对任务进行启动、停止、编辑 等操作。

内容展示:

扫描结束的任务详情页面分为任务统计、漏洞列表、资产列表等多个标签页。

1. 扫描进度:

- 任务正在扫描时,页面会展示扫描的进度,任务扫描的阶段根据扫描策略的不同, 可能包含信息收集阶段和漏洞探测阶段;
- 界面还将展示最近 30 秒的平均响应时间、最近 30 秒的响应失败率;



 若扫描进度长时间不增长,且最近 30 秒的平均响应时间较长、响应失败率较高, 有可能是系统访问被目标防火墙拦截,建议在任务结束后,检查网络连接、目标防 火墙配置是否正常,扫描目标、扫描参数是否填写正确。

fvlsi	統	^{展对比} 扫描历史	▼ 生成报表 5	a 错扫描任务	停止扫描
任务统计 测洞 (0) 域名 (1) 主机 (1) 服务 (1) Web 站点 (1)					
扫描进度		任务基本信息			
	20 (D) (2+0)	任务状态	正在扫描		
	8%	扫描策略	基础 Web 漏洞扫描		
最近 30 秒平均确坚时间为: 1.86ms 最近 30 秒内模型失数率: 0%		启动时间	2021-12-23 18:00:13		
		扫描时长	-00:02:20		
		扫描目标	1		

2. 任务统计页:

任务统计标签页,展示当次扫描结果的统计信息。

 扫描日志:任务扫描结束时,页面会展示扫描过程中的日志信息,可供下载和查看, 如果出现异常可将日志发送给长亭技术支持获取帮助。

fvlsi							结果对比	扫描历史 ▼	生成报表	快速深度扫描	编辑扫描任务	立即日橋
任务统计	漏洞 (0)	城名 (1)	主机 (1)	服务 (1)	Web 姑点 (1)							
扫描日志						下载日志	难更多	任务基本信息				
-					0			任务状态	扫描结束(成120)		
[17:45:44 [17:45:44	45:44] [发现 WEB 站点] http://bruta-force.vul.et:8030/ 45:44] [发现服务] 10.3.0.5:8030 tcp						扫描策略	基础 Web	属洞扫描			
[17:45:44	」(信息收集) (信息收集結)	爬虫已结束探测 束1	•					启动时间	2021-12-23 17:45:38			
(17:46:08) (任务信息)	任务 ID: d94	153bcfff84b3	Bac19bff82e3	79233			扫描时长	0:01:12			
(17:46:11 (17:46:11	3 (高利田湖71) (高利採用) 3 (高利採用)	相〕 自动反连平台失 正在处理 10.3	政,依赖反连平 .0.5:8030	台的幕洞将无法打	325, invalid resp	se from remote reverse ser	vez, 1	扫描目标	1			
[17:46:11) [嘉府探測]	正在处理 10.3	.0.5:8030	-				漏涡插件	588			
[17:46:41	」(高沢採用))(高沢採用)	数据源证取完成 温洞扫描引攀究	,寺侍已有任劳 成扫描	TEAL				已扫描 URL 数量	12			
[17:46:50 [17:46:51 [17:46:51) (廣湖提測語) (状态変更)) (扫描結束)	来) 任务【fvīni】	· 正在扫描 -	· 日福結束 (点)	助), 補出 Wengine			已发出 HTTP 请求数	15			
								已采集 URL 数篇	12			
漏洞数量								推定时间段	÷.			

- 漏洞数量
- 漏洞类型分布
- 服务类型分布
- 任务基本信息



灑洞数量									
	0			 产重 高意 中意 低意 	232 406 316 32			任务基本信息	
漏洞类型分布								红泉树木	扫描结束 (成功)
								社务状态	扫描结束 (成功)
		● 未授权	245	= 其他	229	• 缓冲区	210	扫描策略	基础服务漏洞扫描
		■ 逻辑错误	64	• 信息泄露	54	• 代码注入	50	启动时间	2023-06-16 14:48:56
		· XSS	41	• 整数溢出	24	● 路径遍历	18	扫描时间	0-05-00
		• SQL注入	15	• 密码学	14	意争条件	12	1-0 med tv	0.05.00
								扫描目标	1
								漏洞插件	1
腦务类型分布								存活主机数量	1
		 http 	54	e top	4	 smtp 	3	王的内小社和新聞	
		https	2	• imap	2	• memcac	2	尤明应土机致重	0
		netbios	2	pop3	2	ssh 🗧	2	已扫描主机数量	1
		• zmtp	2	ajp13	31	e amqp	1	指定扫描时段	
		docker	1	• epmd	1	e ftp	1		
		Idap	1	oracle-tns	31	• postgresqi	1	指定禁扫时段	81.

3. 漏洞标签页:

任务统	计漏洞((13) 域名((0) 主机(1) 服务(15	5) Web 站点 (4)								
[洞等级:			漏洞权重:	∨ 漏洞名称:		标签:					查询	H M
+	漏洞等级	漏洞权重	漏洞名称	漏洞影响位置	标签		漏洞状	态				
+	₩.	99%	CVE-2020-1938: Apach	1	原理扫描 WEB 漏洞	HW重点漏洞	• 1	• 0	• 0	• 0	• 0	• 0
+	高危	99%	CVE-2016-2183: OpenS	1	原理扫描 Programmin	ng Language	• 1	• 0	• 0	• 0	• 0	• 0
+	高位	99%	MSSQL 募口令漏洞	1	原理扫描 OWASP_to	p10	• 0	• 0	• 0	•1	• 0	• 0
+	甲度	99%	配置文件泄露-依赖文件	1	原聯扫描 WEB 邏纲	OWASP_top10	• 1	• 0	• 0	• 0	• 0	• 0
+	858	99%	Host头未校验漏洞	1	原理扫描 WEB 講羽	OWASP_top10	• 1	• 0	• 0	• 0	• 0	• 0
+	低魚	99%	HTTP 响应头 X-Powere	1	原理扫描 WEB 識洞	10-1X	• 1	• 0	• 0	• 0	• 0	• 0
+	低應	99%	不安全的密码表单属性	1	康理扫描 WEB 講羽	协议	• 1	• 0	• 0	• 0	• 0	• 0
+	低欣	99%	HTTP 响应头 Strict-Tran	2	原理扫描 WEB 混洞	19-1X	• 2	• 0	• 0	• 0	• 0	• 0

4. 域名标签页:

任务统计 潮湖 (13)	城名 (0)	主机 (1)	服务 (15)	Web 站点 (4)		
18:					30 S	8 R.R.
域名					深间数量	
				智夫政团		
						10 条/页。



5. 主机标签页:

任务统计	漏洞(13)	域名 (0)	主机 (1)	服务(15)	Web 站点(4)		
IP 地址:		响应和	犬态:	Y	操作系统:		重询重置
IP 地址			操作	系统		响应状态	漏洞数量
10.3.0.6			Ubur	itu		存活	1 2 0 0
							< 1 ⇒ 10 条/页 ∨

6. 服务标签页:

任务统计	漏洞(13)	域名 (0)	主机 (1)	服务 (15)	Web 站点 (4)							
端口:		服务类型:			应用:		应用版本:				查询	ÆM
端口		服务类型		应用		应用版本		瀍洞彭				
10.3.0.6:844	43/TCP	https		nginx				173	10		13	
10.3.0.6:443	3/TCP	https		Golang net	http server				•			
10.3.0.6:995	5/TCP	pop3								Þ		
10.3.0.6:800	09/TCP	ajp13		Apache Jse	irv				63		0	
10.3.0.6:993	3/TCP	imap		Dovecot im	apd							
10.3.0.6:465	5/TCP	smtp		Postfix smt	pd					10		
10.3.0.6:808	B0/TCP	http		nginx				0	10			
10.3.0.6:338	89/TCP	ms-wbt-ser	ver	xrdp							0	

7. Web 站点标签页:

任务统计	漏洞(13)	域名 (0)	主机 (1)	服务(15)	Web 站点(4)							
资产地址:		We	b 站点标题:								重询	# M
资产地址				Web	站点标题	url 数量	漏洞數	2量				
https://10.3.	.0.6:8443/			Roun	dcube Webmail :: Welcome to	12				5		
https://10.3.	.0.6/					0	0	0		3		
http://10.3.0	0.6:8080/			301 M	foved Permanently	0	10	0	0	3		
http://10.3.0	0.6/					0	0	0	0	3		
										3	1)	10 条/页 🗸

进行操作:

点击任务详情页面顶部的按钮,可以对任务进行一系列的操作。



● 若当前任务有定期扫描计划,详情顶部展示,点击可以查看计划详情:

每天 17:25:00 定时扫描 下次扫描时间为 2021-10-27 17:25:00 取消任务扫描计划

查看历史扫描结果:

◆ 从任务列表打开扫描任务详情时,默认展示最近一次扫描的扫描结果

fvlsi						结果	对比 扫描历史 🔻	生成报表 快速深度扫描	1111日始任务 立即日指
任务统计	選府 (0)	城名 (1)	主机 (1)	服务 (1)	Web 站点(1)				
扫描日志						下载日志 宣教更多	任务基本信息		
		AN					任务状态	扫描结束 (成功)	
[17:45:44] [发现 WEB] [发现服务]	10.3.0.5:803	brute-force. 10 tcp	.vol.ct:8030/			扫描策略	基础 Web 属羽扫描	
[17:45:44	[信息収集]	爬虫已结束探测	•				0240300	0001-10-03 17-46-98	
(17:46:08) (信息改集日) (任务信息)	(朱) 任务 ID: d94	153bcfff84b3	Bac19bff82e3	79233		With and the first state	EXECTIVE A TRADAGE	
[17:46:08	1 編洞提測开	始」					扫描時代	0:01:12	
(17:46:11) (漏洞探測)	自动反连平台失	致,依赖反连平	台的赢利将无法持	出出, invalid resp	se from remote reverse server, i	扫描目标	1	
[17:46:11	(高洞探测)	正在处理 10.3	.0.5:8030				编课题件	588	
[17:46:41) (蕭將提測)	數据源读取完成	,等待已有任务	完成			and shared in	0.000	
[17:46:42) (温洞探测)	還將扫描引擊完	成扫描				已扫描 URL 数量	12	
[17:46:50	1 [周州田湖田) [状态变更]:	(IN Itvini)	1 正在扫描>	白檀结束(成)	th), WHE Wengine		已发出 HTTP 请求	欧 15	
[17:46:51	1 [扫描结束]							12	
							CONCERNING BOOK	12	
漏洞数量							推定时间段		

● 结果对比:

■ 点击结果对比按钮,跳转到结果对比页面,默认显示最近两次扫描的对比结果;

tvisi			
对比扫描历史	2021-12-23 18:05:25	VS	2021-12-23 18:00:08
任务基本信息对比			
启动时间	2021-12-23 18:06:28	启动时间	2021-12-23 18:00:13
扫描时长	00:01:13	日掘时长	00:01:13
白描目标	1	扫描目标	1
展网数量		漏洞的量	
扫描目标	http://brute-force.vul.ct:8030/	扫描目标	http://brute-force.vul.ct:8030/
左侧扫描历史比右侧扫 增加的服务资产(0)	編历史增加的場务资产、减少约服务资产。相同的服务资产如下表所示 减少的服务资产(0) 相同的服务资产(1)		
MD.	服务类型	应用	应用版本号
NC	服务类型	应用 ————————————————————————————————————	应用版本号
第□ 左照扫描历史比右侧扫	服务类型 描历史增加的主机、减少的主机、有变化的主机、相同的主机如下表所示	在用	应用版本号

● 生成报表:

◆ 在任务详情页可以直接生成该任务(在当前扫描历史下)的报告,报告中不 包含被标记为"误报"的漏洞,正在扫描中的任务无法生成报告。可以选择 等待任务结束、停止任务,或是选择任务一个以往的扫描历史生成报告。



就报表							
*报表名称:	fvlsi的扫描任务报表						
*所属组织单位:	NULTER						
*报表类型:	扫描任务报表						
*报表模板:	扫描任务报表模板						
*报表文件格式:	管理报表模板 図 Word 版 図 Excel 版	✓ HTML版 PDF版					
报表处理:	 按察产聚合 按温粱 	86					
* 860808	点击选择目标扫描任务	an let					清空已选目
"日顿归烟江穷,	扫描任务	所属组织单位	扫描启动时间		扫描状态		操作
	fvisi	默认工作区	2021-12-23 18:05:28		扫描结束	(成功)	810
							< 1
							107 TH 200

- 快速深度扫描:
 - 用于将任务的扫描结果作为目标进行快读扫描;
 - 点击后选择一种扫描模式,然后可以快速选择扫描策略进行扫描。

选择快速深度扫描的模式	×
快速深度扫描是对本次扫描结果中的资产进行快速创建扫 作。	苗任务的一种操
○ 对扫描结果中的主机资产进行扫描	
○ 对扫描结果中的服务资产进行扫描	
○ 对扫描结果中的域名资产进行扫描	
● 对扫描结果中的 Web 站点资产进行扫描	

- 编辑扫描任务:
 - ◆ 在任务详情页可以修改扫描任务的参数配置,编辑扫描任务的方法与添加 扫描任务基本相同,除了任务的扫描策略不可编辑,其他的一切都可以编 辑。



本協會 任务控制	信息收集争数 漏洞投册争数	
E务信息		
	扫描策略名称	基础服务案则打错
	自接筆範構成	
	扫描策略自动同步 ①	
	* 扫描任务名称 ①	#HETHEDongo
	義法	
	* 旧模目标	李动输入 上传出电文件 指定资产组
		183.84
播时间配置		
	* 执行类型	• 立即扫描 定时扫描一次 电天面环扫描 电用脑环扫描 每月期环扫描

- 立即扫描:
 - 启动后,任务可能立即开始扫描,也可能进入等待扫描。这取决于系统当前正 在扫描的任务数量,是否达到了系统的最大任务并发数。

fvlsi		结果对比	扫描历史 🔻	生成报表	快速深度扫描	编辑扫描任务 立即扫描
任务统计 漏洞 (0) 磁名 (1) 主机 (1) 服务 (1)	Web 站点 (1)					
扫描日志	3	下载日志 查看更多	任务基本信息			
			任务状态	扫描结束(6	\$35)	
[18:05:35] [信息收集] 网络 [http://brute-force.vul.ct:80]	07】指纹识别结束		1210/06/08	WER Main I	NACT REPORT	
[18:05:35] [发现曲号] 10.3.0.518030 CCp	0/		12169-04-05	32.00 MeD %	6.45 ST308	
(18:05:35) (信息收集) 爬虫已结束探测。			启动时间	2021-12-23	18:05:28	
(18:05:58) (信息收集结束)			1	1000135		
[18:05:58] [任务信息] 任务 ID: 9c35bc5c5a3b497c86ed1500f	8062b2		口推的代	0:01:12		
[18:05:58] (鳳洞探測开始)			扫描目标	1		
[18:06:01] [黨兩探測] 启动反连平台失败,依赖反连平台的漏洞将无	問出出, invalid response from remote re	verse server,)				
[18:06:02] (満洲営業) 社会定理 10.3.0.5:8030 110.05.123 (開始営業) 教授等決的定点 第5日本は希定成			面洞插件	588		
110:06:321 (憲法時間) 数据目標可要完成目標			PDB UR NO	11		
[18:06:40] [圖湖探測結束]			CTINES OF A MORE			
[18:06:41] (状态受更)) 任务 [fvts1] : 正在扫描 -> 扫描结束 ;	或功), 陳因: Wengine 消息		已发出 HTTP 请求数	15		
[18:06:41] [扫描結束]			已采集 URL 数量	11		
道河参議			指定时间段			

● 停止扫描:



visi	结果)	时比 扫描历史 🔻	生成报表 編輯出譯任為 醫學任表 參上扫描
任务统计 漏洞 (0) 端名 (1) 主机 (1) 服务 (0) Web 站点 (1)			
推进度		任务基本信息	
		任务状态	正在扫描
1650.8	0%	扫描策略	基础 Web 運用扫描
最近 50 形平共明白时间为: 0ms 最近 30 称内调和无效率: 0%		启动时间	2021-12-24 10:36:29
		扫描时任	-00:02:27
		白檀目标	3
贈日本 下数日本	重要更多	展测组件	588
		已日樹 URL 数量	0
(10134-29) (信息收集) 正在初始化肥金定例		已发出 HTTP 请求题	0
[10:36:29] [10:00()] 正住10() #80 田戸 & SAN ATAN [10:36:29] [信息収集] 接收到扫描目标: [http://brute-force.vul.ct:0030/]		已采集 URL 数量	0
(10:36:29) (変現 WEB 页页) http://hrute-force.vul.et:8030/		40 CD 6+421115	
(10:36:29) [波現 WEB 地点) http://brute-force.vul.ct:8030/1 世行地站2868		228.942.942.642.648	
[10:36:29] [发现综合] brute-force.vul.ct			
[10:36:29] [宏地 WEB 用面] http://brute-force.vul.ct:8030/login/get (10:36:29) [御服 WEB 回面] http://brute-force.vul.ct:8030/login/post-redirect			
[10+36+29] [发现 WEB 页页] http://brute-force.vul.ct/8030/login/post-check-referrer-single-pass			
(10:36:29) (发现 WEB 页面) http://brute-force.vul.ct:8030/login/basic-auth			
[10:34:30] [信息収集] 发现新的得出主机: 10.3.0.5			
110.35.361 (単位十位) () () 5 5 5 5 () () () () () () () () () () () () ()			

- 暂停漏洞检测【被动 Web 扫描(代理/日志)特有操作】:
 - 暂停漏洞检测,系统只进行信息收集,不进行漏洞检测;
 - 暂停信息收集,系统会继续检测漏洞,但不会进行信息收集;
 - 继续漏洞检测,可恢复漏洞扫描引擎工作。

被动Web扫描代理测试101 -	结果对比	扫描历史 👻	生成报表 🥼	種目描任务	醫療信息收集 停止扫描
任务统计 漏洞 (0) 域名 (0) 主机 (0) 服务 (0) Web 站点 (0)					
扫描进度			任务基本信息		
语连接以下 HTTP 代理进行信息变靠: 10.2.19.11 使用 HTTP 代理后可能会影响有户端使用 HTTPS 的网站,下载 HTTPS 概证书并安装可解决该问题。		0%	任务状态 扫描策略 応設印面	正在扫描 被动 Web 扫描(代理) 2021-12-24 10:38-19	
最近 30 秒平均确定时间为: Gms			白猫时长 扫描目候	-09:02:21 1	
扫描日志	下载日志	宣看更多	漏調插件 已扫描 URL 數量 已发出 HTTP 请求数	588 0	
[10:39:16] (式空変): 任务 [後近986日通代運動法01] + 等待用期 → 等待日請。周田: 手动操作 [10:29:19] (式空変): 任务 [後近986日間代運動法01] + 等待日請 → 正在日路。周田: 并发控制件可 [10:39:19] (日茶店約) [10:39:19] (日茶店約) (日茶: 10: e0:011500e316cd9865114716373e35 [20:39:19] (日茶店約) (日茶): e0:011500e316cd9865114716373e35 [20:39:19] (信約成為) (日茶店約) (日本): e0:011500e316cd9865114716373e35 [20:39:19] (信約成為) (日本): e0:011500e3164cd9865114716373e35 [20:39:19] (信約成為) (日本): e0:011500e3164cd9865114716373e35 [20:39:10] (日本): e0:011500e316400e3164cd9865114716373e35 [20:39:10] (日本): e0:011500e3164cd9865114716373e35 [20:39:10] (日本): e0:011500e3164cd9865114716373e35 [20:39:10] (日本): e0:011500e316400e3164000300000000000000000000000000000000			已深集 URL 數量 指定时间段	0	
10:39:20 (高思攻集) 包連 mrar 代理成功 10:39:24 (高思攻集) 开始接收信息収集法集					

- 资产趋势分析【主机资产监控特有操作】:
 - 正在扫描的任务展示发现资产的趋势分析结果与最近两次监控结果的对比
 - 展示最近9天的存活主机数量趋势分析、服务数量趋势分析、不同风险等级的 漏洞数量趋势分析
 - 点击右上角的返回最新监控结果跳转到详情页展示内容在扫描结束的任务详 情基础上多出扫描进度



test						资产趋势分析	扫描历史 •	生成报表	快速深度扫描	编辑扫描任务	立即扫描
■ 毎天 10	49:00 定时扫描	下次扫描时间)	ካ 2021-12-25 1	0:49:00						B 28	任务扫描计划
任务统计	漏洞 (0)	城名 (0)	主机 (1)	服务 (29)	Web 站点 (8)						

			The second second second				Last Del Nel 1	
5.425.800	± et.es.ax 1		29		8	0	E-MLAX BX	07
存活主机数量趋势分	ff							
存活主机数量								
1								
0.75								
0.5								
0.25								
0 / 2021-12-17	2021-12-18	2021-12-19	2021-12-20	2021-12-21	2021-12-22	2021-12-23	2021-12-24	2021-12-2
服务数量趋势分析								
服务数量								
32								
24								
16								
8								
0 10 17	0001 10 10	0001 10 10	1001 10 00	0001 10.01	0001 10 00	0001 10.00	0001 10.04	2021 12

test					返回最新版控结果
趋势分析 量近两	次监控结果对比				
对比扫描历史				VS	
任务基本信息对比					
77					
资产结果对比(左侧扫描	(历史比右側扫描历史)				
左侧扫描历史比右侧扫描	历史增加的服务资产,减	少的服务资产,相同的服务	杨资产如下表所示		
增加的服务资产 (0)	減少的服务资产(0)	相同的服务资产(0)			
- 左侧扫描历史比右侧扫描	历史增加的主机、减少的	主机、有变化的主机、相同	同的主机如下表所示		
增加的主机资产(0)	减少的主机资产 (0)	相同的主机资产 (0)			
-					
漏洞结果对比					
左侧扫描历史比右侧扫描	历史增加的漏洞、减少的	贏洞,相同的漏洞如下表 ^向	fiat		
增加的漏洞(0) #	业少的漏洞(0) 相同的	調測(0)			



3.1.4 扫描设置

在左侧导航栏中,选择"扫描管理-扫描设置",选择要设置的方向,进入对应的界面。

工作区 🗸	13月前年 /	四田以王 / 字典管理					
全局仪表盘	(HAR)	NINE WAINS ×	+ 酒加锦选条件				
通管理 ヘ	0 8	选择 0 个字典 🛛 📰 🔅	eastern.				+ 383a
任何统计		字典名称	字典内容	字典类型	创建单位	字典最后更新时间	細作
任务对象		Zabbix 用户名字具	其包含1行	用户名字典	8	2021-11-25 10:49:21	28
B#81 *		Zabbix 密码字典	共创造1行	肥码字典	41	2021-11-25 10:49:21	-
学校管理	- 63	WebLogic 用户名字画	共恒省1行	用户名字典	97 27	2021-11-25 10:49:21	-
建口经管理		WebLogic 图码字典	具物含 4 行	肥码字典	7 5	2021-11-25 10:49:21	
重打夺台道听配置		WebBasic 用户名字典	共物合 5 行	用户名字典	10	2021-11-25 10:49:21	-
紙管理 ッ		WebBasic 图码字典	共包含 14 行	密码字询	43	2021-11-25 10:49:21	22
PΦ0 ~		VNC 用户名字典	其包含 0 行	用户名字典	ŝĩ	2021-11-25 10:49:21	
同管理 ~		VNC 密码字典	共物含年行	肥码字典	8	2021-11-25 10:49:21	
84 ×		Teinet 用户名字具	共包含 5 行	用户名字典	81	2021-11-25 10:49:21	
- IF IF IF		Teinet 密码字典	其包含 9 行	密码字典	90	2021-11-25 10:49:21	
- EE				i di c	2 3 4 5	6 7 3 30.4/8	28.97

3.1.4.1 字典管理

字典可以方便您更好地通过添加自定义字典进行扫描过程的定制。

内容展示:

字典列表为您展示所有字典的基本信息:

<・>洞₩x-не									admin
默认工作区	v in	estera 7.1	11月1日(二字奏管理						
♀ 全局保表盘		(man	1991 就以工作区 X	+ 漬加神送条件					
in energy		0 Ei	5择 0 个字典					■虹膜操作 〜	十期初一个年期
任务统计		6	学典名称	字典内容	命中次数	字典类型	包建单位	字典最后更新时间	NA15
扫描的	2		Zabbix 用户名字典	共包含1行	0	用户名字典		2022-12-14 15:19:28	20
H-RPIA EMWX			Zabbix 密码字典	共包含1行	0	密码字典	(4)	2022-12-14 15:19:28	
7828			WebLogic 用户名字典	具包含1行	D	而户名字具	121	2022-12-14 15:19:28	
油口绘教理			WebLogic 图码字典	共包含 4 行	0	密码字典	152	2022-12-14 15:19:28	28
全地在老早配置			WebBasic 用户名字典	共告告 5 行	۵	用户名字典	(*)	2022-12-14 15:19:28	
第打平台追听配 算	¢.		WebBasic 密码字角	共包含 14 行	0	思码字典		2022-12-14 15:19:28	8.8
A 基础管理	÷		VWC 用户名字典	共包含 0 行	0	用户名字典		2022-12-14 15:19:28	28
き 資产中心	-		VNC 图码字牌	共能含 9 行	o	密码字典	141	2022-12-14 15:19:28	
☆ 運動管理	*		Telcet 用户名字典	共铝含 5 行	0	用户名字具	1.50	2022-12-14 15:19:28	-
直 接書中心			Teinet 密码字典	共包含 9 行	o	度码字典	2.53	2022-12-14 15:19:28	
LI RIER								6 7 5 10.82	1 IN 22 IN
· same									- ma 14



• 字典内容,展示字典内容的总行数:

<·>洞鉴x-₽	AY							admin
默认工作区	v 1	1889年(1989年(李貞登現						
2 全局仪表盘		(REEROD MUITE X)	+ 液加弹选条件					
13 白昏世祖	*	● 已选择 0 个字典	i包含 1 行, 總要预定: dmin				批業操作 ~	+ 酒誌一个学典
任务统计		- 788R	****	命中次数	字典类型	创建单位	字典最后更新时间	操作
扫描策略		Zabbix 用户名字典	共在含117	0	用户名字典	-	2022-12-14 15:19:28	24
任务约束		Zabbix 图码字典	共包含1行	0	密码字典	÷.	2022-12-14 15:19:28	
7A28	1	WebLogic 用户名字典	共包含1行	0	用户名字典		2022-12-14 15:19:28	
		WebLogic 密码字角	共回告 4 行	0	密码字角	-	2022-12-14 15:19:28	28
全局白名单配置		WebBasic 用户名字商	共包含 5 行	0	用户名字典	2	2022-12-14 15:19:28	24
有 打平台盖明配	я	WebBasic 图码字典	共包含 14 行	0	密码字典		2022-12-14 15:19:28	28
A MARTIN	~	VNC 用户名字典	其包含の行	0	用户名字典		2022-12-14 15:19:28	
5 2740	*	VNC 密码字典	共配當 9 行	o	密码字典	2	2022-12-14 15:19:28	
△ 派羽管理	٣	Teinet 用户名字类	共包含 5 行	0	用户名字典	-	2022-12-14 15:19:28	-
道 服務中心	*	Teinet 密码字典	共包含9行	0	密码字典	-	2022-12-14 15:19:28	
C) 9019/8	Ť							_
③ 系纹器理	Ψ.					1 2 3 4 6	6 7 > 10 条/到	※ 施至 页

查看字典:

在字典管理页面可点击字典条目查看字典内容;可以一键复制字典内容;对字典的 命中次数进行清零操作。

基本信息				
字典名称	Zabbix 密码字典	字典创建人		
字典来源	系統内置	字典创建时间	2022-12-14 15:19:28	
字典类型	密码字典	字典最后更新时间	2022-12-14 15:19:28	
命中次数	0 归零			
字典内容 一键的	夏制字典内容			
zabbix				

筛选字典:

 在字典管理页面可顶部可以添加筛选条件并保存,筛选维度为字典名称、所属组织 单位、字典类型与字典最后更新时间;可以在页面顶部或者筛选弹窗中删除已经设 定的筛选条件

添加字典:

在字典管理页面可以添加字典。



 填写、选择、上传字典的具体信息如图:字典名称是字典的标识,不能和已有的字 典名称重复;上传字典文件大小不能超过 10M;

添加一个字典		×
* 字典类型 ①	其他字典	
•字典创建单位 ①	默认工作区	
• 字典名称	请输入长服为 1-32 个字符,且不信含	空格的字典
* 字典文件		
	点击或将文件指搜到这里 文件大小不超过 10 M	上传

删除字典:

● 在字典管理页面可以批量删除已有的字典。

main	0.5+6 请不要删除测试数据	× + 道加祥选条件					
0 8	1选择 2 个学典					杜鹃路作 -	+ 8%-17
	字典名称	子典内容	命中次数	7A21	创建单位	7A	18.17
	2	共租金支行	0	其他学典	這不要倒除意識飲留	2023-04-04 11:15:37	
	23021010	共居合 11 任	2	其他学典	请不要删除测试数据	2023-04-04 11:06:09	
	空行测试	共包含 6 行	0	其他学典	请不要删除测试数据	2023-04-10 17:20:31	
	定时发	共包含 2 行	0	其他学典	纳不更删除测试数据	2023-03-15 11:52:28	
	mina	共包含 2 行	2	能码字典	请不要删除测试数据	2023-04-06 15:53:53	
	依方去条义律个干息	共恒会7行	2	其他学典		2023-03-15 13:29:23	

编辑字典:

 自定义的字典可以进行编辑操作:字典内容支持空格或空行为空口令,如果输入多 个空行,点击确定后只保留第一个空行为空口令。

相子典		×
•李興清堂 ◎	其他学典	
************	默认工作说	
* 字典名称	[nodel] 能证mysg沉存在空格	
* 字典内容	Makenggenowiel	



3.1.4.2 端口组管理

端口组可以方便您更好地进行扫描过程的端口组的定制,您可以在此处进行端口组 的预览、添加和删除。

2127年(1998年) 第四相管理			
(MRESHO MUITR X)	+ 添加渐选条件		
 已选择 0 个扫描端口组 		杜爾姆	s ~ 🛛 + 353
端口坦名称	第口告诉派	创建单位	編口組更新时
数据库端口组	提供了数据库常用端口	÷	2023-04-18 10
Web 08⊡18	提供了 Web 常用端口	°	2023-04-18 1
UDP 常用错口组	提供了 UDP 常用端口组	*	2023-04-18 11
TCP 常用第口组	据供了 TCP 常用端口细	¥.	2023-04-18 18
IN I	提供了 TCP Top 10 備口	ē.	2023-04-18 18
			115

内容展示:

端口组列表为您展示所有端口组的名称,端口组描述、创建单位、端口组更新时间。 对端口组列表可进行筛选、删除和编辑操作。注意:内置的端口组不可编辑和删除。

添加端口组:

- 在扫描端口组列表页面,可以添加自定义的端口组。
- 端口组名称,添加或编辑主机扫描任务时,若要从端口组添加需要扫描的端口,端口组名称是用户能够看到的唯一信息,请务必填写一个容易分辨的端口组名称;
- tcp /udp 端口组,端口组中包含的 tcp/udp 端口:
 - 可以输入单个端口或端口段,如:80,10-20,也可同时填写多个端口或端口段, 端口或端口段之间换行分隔,如下图中所示。

添加扫描端口组	×	
* 端口组名称	请输入递口组名称	
端口组描述	请输入馈口组描述	
*端口组创建单位 ①	默认工作区	~
tcp 端口组	狼行分隔, 输入档式如下: 80 10-20	
udp 端口组	执行分隔,输入格式如下: 80	
		l


3.1.4.3 全局白名单配置

全局白名单配置页面可以添加配置和管理可应用于多个不同任务的全局白名单,可 对添加的白名单进行查看、编辑、删除操作

<♪洞鉴x-RAY									admin
默认工作区 >	∃損管理 / 非	1819 1 全局白名单	配置						
◎ 全局仪表盘	- Filler	单位 默认工作区 ×	+ 激加筛选条件						
□ 扫描管理 、	0 已选	择 0 个扫描白名单					批量操作 >	+	添加白名单模板
任务统计	Ū*	白名单名称	白名单撮述	所属组织单位	创建用户	最近更新时间		操作	
扫描策略		默认+不漏洞		默认工作区	admin	2022-10-21 10:12	:28	요즘	16111 Bills
任务列表	- 0	@! #¥%	1	默认工作区	admin	2022-10-13 19:41	:51	立者	NATE BOOK
行推议置 ^	0	我一个三十二		默认工作区	admin	2022-10-21 10:12	:57	25	10.11 HIZE
端口相管理		手动添加白名		默认工作区	admin	2022-10-13 19:57	:09	24	inia mat
全局白名单配置		2	R.	默认工作区	admin	2022-10-13 19:58	:00	宜看	skitl Bills
盲打平台监听配置		tcp+urilele	12	默认工作区	admin	2022-10-14 18:37	:12	宜着	igiti Bitt
▲ 基线管理 ~	0	233		默认工作区	admin	2022-10-18 16:16	:15	皇君	sent men
◎ 荒产中心 ~	0	8	8	默认工作区	admin	2022-10-18 16:51	:10	25	inti mut
る 漏洞管理 ジ		~! @#¥%	*	默认工作区	admin	2022-10-18 16:53	:11	宜者	编辑 删除
自 报表中心 ~									

添加白名单:

可以添加白名单名称、描述、所属组织单位、信息,导入或者添加想要规避的扫描 目标。注意只能导入所属组织单位以及其子单位的主机/Web 资产。同时可以编辑规避 扫描的 URL 关键字。保存后可以应用到扫描任务。



(•)洞螢 _{X-R} /									
此认工作区	v		11111日 / 全局白名单	尼查		添加扫描白名单			5
2 全局仅表量	1	市業組织	#位 默认工作区 X	+ 添加筛选条件					
日日間管理	8	0 已选	择 0 个扫描白名单			基本内容			
任务统计			白名单名称	白名单描述	所属组织单位	* 白名单名称	请填写白名单名称		
扫描策略			默认+不漏洞	-	默认工作区	白名单描述			
任务列表			o: #¥%		默认工作区	*所属组织单位 ③	默认工作区		
字典管理			我一个三十二		默以工作区	规避扫描的目标 ⑦	白名单格式,固车换行 host.com*.website.com	與行分隔 .com1.1.1.1https://www.	
字典管理 第口组管理			手动添加白名		默认工作区		chaltin.cn/https://www 目标白名单为类似 http://down.wil.ct-902	ww.chaitin.cn/admin+若	导入 Web 资产
全局白名单配置			2		默认工作区		id=18Submit=Submit ??后的内容,或者用	的形式,请不要省略	
盲打平台 <u>當</u> 听配]	ĸ		tcp+urilele	•	默认工作区		http://dvwa.vul.dt:9020	2"代替	
4基线管理 、	8		233		默认工作区	扫描白名单适用 ⑦	🛃 不进行资产发现 😔	不进行罵問检測	
自产中心 ·	8		å		默认工作区	高级配置			
) 進羽管理 、	8		~! @0¥%	\$	默认工作区	URI 禁扫关键字	delete × remove ×	logout ×	
报表中心	8								取消 🕅

全局白名单应用于全局:

"应用配置"开启后,该工作区的任务会在下一次扫描时应用全局配置,勾选"同步应 用到子工作区"可将此全局白名单配置同步应用到子工作区。若当前开启了全局白名单 的应用配置,那么该版本后创建的任务首次/再次开启扫描任务时,会应用全局配置。 一个工作区可存在多个全局白名单,支持开启多个,支持任务应用多个。

* 白名单名称	请填写白名单名称	
	不是有效的白名单名称	
白名单描述		
*所属组织单位 ⑦	默认工作区	v
规避扫描的主机目标 ⑦	1.1.1.1/24 [1234::0] 1.1.1.1:90 1.1.1.1:90,100 1.1.1.1:90,100 1.1.1.1.1:2:90 [1234::0]:90 :90	导入主机资产
規避扫描的 Web 目标 ⑦	白名单格式。回车换行分隔 http://www.website.com/ https://www.website.com/admin+ 若目标日名母为类级 http://dwwa.vul.ct:9020/7 id=1&8Jubmite.Submit 的形式,请不要省略"7后的内容,或者 用 http://dwwa.vul.ct:9020/* 代替	导入 Web 资产
扫描白名单适用 ⑦ 开启应用配置,该工作 下一次扫描时应用全质 置同步应用到子工作取	✓ 不进行资产发现 → 不进行展测检测 F区的任务会在 起置: 可将配 nove × logout × K	

3.1.4.4 盲打平台监听配置

部分插件需要反向连接才能够确定漏洞,如存储型 XSS、文件上传、SSRF 等。此 处可以为这类插件提供监听 IP 的配置,分为内置盲打平台和外链盲打平台。

内置盲打平台配置:

如果扫描目标与洞鉴服务器可以互相通信,那么仅需配置内置盲打平台即可。此处 监听 IP 地址是洞鉴服务器的 IP 地址。

111211012	獻以工作区 ×) + 淡加線造条件						
E选择 0	个审打平台					ELMINT v	重加實訂平會
	平台名称	푸승백년	所戴组织单位	#10	Hill?		
	內禦軍打平台	http://10.2.28.144:12345 vmi//10.2.28.144:12346		内面	10.10		
	制打平台11	140pc//10.8.33.142:55555 mmc//10.9.33.142:55555	WUITHE	自定义添加	14410 MIR.		
	第 打平台12	http://10.9.33.142:55555 (mic//10.9.33.142:55555	献说工作区	假定义添加	1010 810		
	第77 平台13	http://10.8.33.142:55555 mtl://10.8.33.142:55555	默认工作区	四定义清加	1610 858		
	重打平台14	Mtp://10.0.33.142/55555 mti//10.9.33.142/55555	MULTRE	R22.55	1010 872		
	兼打平台15	http://10.9.33.142:55555 mt//10.9.33.142:55555	MATAR	07.588	1410 850		
	窗打平台16	Http://10.0.33.142:55555 mm://10.0.33.142:55855	MUIME	能建立活动	1611 812		
	BEN R	101p://123:22 +	WULDE	四次火港加	10.12 0.00		
	一个會打	http://12312:222 [-	NULTE	自定义添加	NAME AND		
	窗灯平台18	http://10.8.33.142:55665 mici/10.8.33.142:55655	默认工作区	自定义清加	10112 202		

配置内置盲打平台 IP 地址:

初次配置监听 IP 的步骤如下:

- 确认洞鉴服务器的地址,保证可以被扫描目标访问到,作为内置盲打平台 IP 地址:
- 在盲打平台监听配置处, 输入 IP 地址。

修改内置盲打平台 IP 地址:

"编辑"操作可修改内置盲打平台的 IP 地址。

外链盲打平台配置:

如果扫描目标与洞鉴服务器不能互相通信,则需要在与两者都可通信的地方自行部 署盲打平台,并在此进行配置。

添加外链盲打平台:

● 点击"添加盲打平台",填写以下相关信息(token、HTTP 服务、RMI 服务 的配

置参数见下文中的"外链盲打平台部署说明"):

- 盲打平台名称:用于扫描任务配置的选项;
- 组织单位:仅该组织单位下的用户可在扫描任务配置中使用该盲打平台;仅该 组织单位的负责人能够编辑和删除已添加的外链盲打平台;
- 通信 token: 作为通信认证依据;
- HTTP 服务:按照提示格式填写 http 服务通信地址;
- RMI 服务:按照提示格式填写 RMI 服务通信地址。
- DNS 配置
 - ◆ DNS 服务器域名
 - ◆ DNS 服务器 IP

为存储型 XSS 引擎默认会引	i、SSRF 等一切需要5 用内置盲打平台,如骤	(向连接才能确定漏洞的插件提供的配置,监听 IP 地址 [对引擎特殊配置,请点击前往 <mark>配置引擎盲打平台</mark>	是本系统服务器的 IP 地址,需要保证以下	篮听 IP 地址可以被扫描目标记	[何至]
(所属组织单) ● 已选择	2 默认工作区 X) 0 个盲打平台	+ 添加筛送条件			批量操作 > 添加盲打平台
	平台名称	平台地址	所罵組织单位	类型	操作
	内置盲打平台	http://10.2.28.144:12345 mii://10.2.2		内置	编辑

修改外链盲打平台:

权限说明:编辑和删除仅限该盲打平台所属工作区的负责人操作。

● 同修改内置盲打平台,点击操作列的"编辑"按钮,即可修改。



<→洞鉴	X-RAY					-		admin
默认工作区	×	- 約翰敦現 (約	3個演算 2 賓打平台當會	行動調		添加外链盲打平台		×
* 全府仅表盘 日 白服新闻 任务机计	*	为存储型 X 引擎取认会 一州风田町	KSS、SSRF等一切需要 201月内重音打平台,如 1940 默认工作医 X	反向连接才能确定加测的结件提供的配置。 据时引擎特殊配置,确点由前往 和面创攀 + 通加转送条件	篮听 P 地址是本系统座务器 實打平台	* 盲打平台名称 * 组织单位	请能入面打平台名称,用于任务配面时选择 不是有效的面打平台名称 默以工作区	
白适原格		• Cit	择 0 个實打平台			* 通信 Token		
任务判款	•		平台名称 内置宣打平台	平台地址 http://10.9.33.32:12345 j mii//10.	DNS 配置	* HTTP 服务	不是有效的通信 Token http://t.2.3.4.1234 不是有效的 HTTP 服务	
字典管理						RMI 服务	mii//1.2.3.4:1234	
端口相關 全用白名	2 中記版				x-Ray XR-50-6 10-22 12:001.	DNS 配置 ⑦		
重打平台	ana.					* DNS 服务器域名	DNS 編影器域名不能为空	
A ROAD	-					* DNS 服务器 IP		
意 治产中心	×						DNS 服务器 IP 不能为空	
0 風雨田道	ų.							
· 指表中心	×							
CI ADDAR								
© 5.0%#	~							取消 领定

外链盲打平台部署说明:

外链盲打平台使用步骤:

- 下载盲打平台客户端(联系技术支持人员获取),在需要部署的服务器上启动;
- 通过命令行,启动盲打平台的 http、rmi、dns 服务,设置通信 token;
- 在洞鉴系统上,"扫描管理-扫描配置-全局配置"处,添加外链盲打平台,并将2中
 设置的 http、rmi、dns 和 token 按规定格式填写并保存;
- 创建扫描任务时, 盲打平台配置处启用上述设置的盲打平台即可。

启动服务使用说明:

GLOBAL OPTIONS:	
http-listen value	start a http reverse service, eg. 127.0.0.1:1111
rmi-listen value	start a rmi reverse service, eg. 127.0.0.1:2222
server-ip value	IP address of the server, used to configure dns
domain value	dns domain, eg. xxxxx.com
domain-name-server	Whether to set the server to name server
token value	reverse service token
dbpath value	set the db path
config FILE	load config from FILE
version, -v	print the version



样例说明:

只启动 http 服务的反连平台

./reverse --http-listen 0.0.0.0:1111 --token aabb

启动 http 和 rmi 服务

./reverse --http-listen 0.0.0.0:1111 --rmi-listen 0.0.0.0:1099 --token
aabb

手动设置数据存储位置

./reverse --http-listen 0.0.0.0:1111 --token aabb --dbpath ./save.db

由于现在添加了 DNS 的配置,所以推荐使用配置文件进行启动,启动样例如下:

./reverse --config conf.yaml --dbpath a.db

其中 conf.yaml 的内容如下:



当然也可以使用如下参数命令行启动。

./reverse --http-listen 0.0.0.0:1111 --domain xxxxx.com --domain-name-server true --token aabb



其中的 domain 是准备好的反连的配置好的域名, domain-name-server 的参数配置是 代表是否修改了域名的 ns 为反连平台,如果是,那 nslookup 等就不需要指定 dns 了,也就是可以直接 ping+域名进行漏洞验证。

dns 反连平台配置准备工作:

云服务器

Ubuntu 20.04

安全策略:开启反连平台对外端口,开启 53 端口(UDP 协议)

也就是修改安全组策略,将 53 端口开放, 注意,协议类型一定要是 UDP

问规则	1 导入安全组	1规则 占 导出 !	②健康检查				
入方向	出方向						
手动添加	快速添加	Q 输入端口	或者授权对象进行搜索	不合并		×	
授权策略	优先级 ①	协议类型	端口范围 ①	授权对象 ①	描述	创建时间	操作
						2022年10月24日	编辑复制

然后将需要对外开放的,部署反连平台的端口进行开放,比如 8777, 注意,该端口 的协议类型是 TCP

访问规则	上 导入安全组	且规则 占 导出 (◎健康检查				
入方向	出方向						
手动添加	快速添加	Q、输入端口	或者授权对象进行搜索	不合并		\sim	
授权策略	优先级 ①	协议类型	端口范围 ①	授权对象 ①	描述	创建时间	操作
🗌 🥥 允许	1	自定义 TCP	目的: 8777/8777	源: 0.0.0.0/0		2022年10月26日 10:21:28	编辑 复制 删除
🗌 🎯 允许	1	自定义 UDP	目的: 53/53	源: 0.0.0.0/0		2022年10月24日 14:08:08	编辑 复制 删除



解决 53 端口被 systemd-resolve 占用的问题

首先使用以下命令确认端口占用情况

sudo netstat -nultp

在确认被占用后,可以执行如下命令停用 systemd-resolved

sudo systemctl stop systemd-resolved

编辑 resolved.conf

sudo vim /etc/systemd/resolved.conf

将文件中的对应内容改为如下内容

[Resolve]	
DNS=x.x.x.x	#取消注释,增加 dns,此处的值可以填写你的云服务器公网 IP
#FallbackDNS=	
#Domains=	
#LLMNR=no	
#MulticastDNS=no	
#DNSSEC=no	
#DNSOverTLS=no	
#Cache=no-negative	
DNSStubListener=no	#取消注释,把 yes 改为 no
#ReadEtcHosts=yes	

修改完成后运行如下命令即可解除占用

sudo In -sf /run/systemd/resolve/resolv.conf /etc/resolv.conf



域名

以下的 ip 请替换为准备好的云服务器的公网 ip

1. 仅配置如图所示的内容:

	主机记录 :	记录类型 :	线路类型 ;	记录值 ÷	权重	= MX ÷	TTL :	最后操作时间 :			操作	
•	ns1	A	默认	8.130.41.223	-	-	600	2022-10-18 11:34:53	п	œ	SSL	Ū
•	ns2	A	默认	8.130.41.223		-	600	2022-10-18 11:34:52	п	œ	SSL	Ū

不做其他任何变动,同时配置文件填写好,在启动后,支持 http/rmi 的反连, dns 仅支

持在使用 dig 或者 nslookup 时,指定 IP 解析的情况下,接收到请求。

也就是说,执行 ping/curl 命令时,反连平台并没有办法收到 dns 解析记录。

如果想要让反连平台的 dns 功能也正常工作,应进行如下操作:

腾讯云

1. 自定义 DNS Host

(- jarci	s-cy.fun								9	信小程序	000	大得帮助
概览	实名认证	域名安全	域名转移	自定义 DNS Host	操作日志							
自定义 DN	IS Host, 是指银	用当前域名创建 DM	NS 服务工,由自	己创建的 DNS 服务器提供	t DNS 解析服务。该功能	需要一定专业知识。	不了解的情况下请勿使	E用。				
如果以下口	DNS Host 用来自	RHT jarcis-cy.fun, j	的必在对应域名	S服务器上添加对应 A 记录	(IP 地址保持一致)。							
添加 DNS	Host	司步 DN9 Host										
DNS Host	6		IP 地址	£		級作						
ns1	-		→ 8.130.	41.223		修改 影除						
ns2	-		8.130.	41.223		修改 删除						

2. 修改域名的 DNS 解析



览 实名	认证 域名安全	全 域名转移	自定义 DNS Host	操作日志
基本信息				
成名	internet date			
城名类型	New gTLD			
注册商	烟台帝思普网络科	料技有限公司 (1)		
续费	解析下	戰域名证书		
DNS 解析)			
DNS 服务商	其他			
域名停靠	未启用 前往DNS	SPod管理 🗹		
DNS 服务器	ns2. ns1.			

3. 修改完成后, 需要 10 分钟到几小时不等的时间生效, 时间越久, 部署效果 越好

阿里云

1. 自定义 DNS Host



0 вахом, данновлялание спочала, авсовлочая валиная, насмая	eraatontee, mittonoom, toto	
EMERAL RE		
曹蒙提示: 如果以上ONG 服务副用单解析 scratronest.ext,请告诉在以上对应将名服务副上包30时间 A 记录 (# 185		



2. 修改域名的 DNS 解析



准备好后,即可将工具上传上去,将准备好的域名填写上去即可

注意事项:

- http 服务必须启动,由于远程 server 通过 http 服务来做数据交换,不设置会直接报错;
- token 需要保持和服务端一致,这样才能正常通信;
- dbpath 如果没有指定,会将数据存在临时文件内,它是一个简单的 kv 数据库,其
 作用是用来存储反连数据,可以做数据持久化。

3.1.5 添加扫描任务

添加扫描任务入口:

- 在扫描任务列表页点击 "+ 添加扫描任务", 即可添加一个扫描任务。
- 在扫描策略列表,每个扫描策略右侧,点击"扫描",即可快速创建一个扫描任务。
- 在资产列表中,选中多个主机资产/web站点/资产组,可针对特定的资产下发扫描
 任务。
- 在知识库-漏洞库中,选中多个漏洞,可针对特定的漏洞类型下发扫描任务。

扫描参数配置:

详情见对应的以下各个扫描策略模板参数配置说明

Web 漏洞扫描:



- 主动 Web 扫描:
 - 基础 Web 漏洞扫描-模板参数配置
- 被动 Web 扫描:
 - 被动 Web 扫描 (代理) -模板参数配置
 - 被动 Web 扫描 (日志) -模板参数配置
 - 被动 Web 扫描 (镜像) -模板参数配置
 - 被动 Web 扫描 (kafka) 模版参数配置
 - 被动 Web 扫描 (burp) -模板参数配置

系统漏洞扫描:

- 主动系统漏洞扫描:
 - 基础服务漏洞扫描-模板参数配置
 - 特定服务扫描-模板参数配置
- 被动系统漏洞扫描:
 - 被动服务扫描(镜像)-模板参数配置

资产发现与监控:

- 主机资产监控-模板参数配置
- 域名资产发现-模板参数配置
- 被动资产发现 (镜像) -模板参数配置

逻辑漏洞扫描:



● 逻辑漏洞扫描-模版参数配置

参数配置完成添加任务

- 扫描任务参数配置完成后,点击"创建并立即扫描任务"或"仅创建任务",即可
 完成扫描任务的添加。
- 若点击"创建并立即扫描任务",则创建任务,同时会立即按配置好的参数 扫描任务。
- 若点击"仅创建任务",则仅创建任务,但不做扫描操作

由资产批量添加扫描任务

由资产批量添加扫描任务时,系统会根据资产所在的组织单位,自动分配对应可选的引擎节点,并只提供快速下发入口(无法配置详细参数)。

3.1.5.1 基础 Web 漏洞扫描

可对 Web 站点进行基础主动的漏洞扫描。

- 扫描目标: Web 站点地址。
- 适用场景:需要对特定的 Web 站点资产进行基础的风险检测。

基本信息

- <u>任务信息</u>
- 扫描时间配置
- 全局白名单选择
- <u>引擎节点选择</u>

任务控制

- <u>扫描优先级</u>
- <u>扫描任务限制</u>
- <u>HTTP 客户端限制</u>
- <u>扫描白名单配置</u>
- 自动生成扫描列表
- 扫描动态通知



• <u>扫描结果处理方式</u>

信息收集参数

- <u>HTTP 请求配置</u>
- <u>HTTPS 客服端证书</u>
- HTTP 基础认证
- Web 表单登录
- 网站可用性验证
- Web 爬虫
- <u>目标采集</u>文件
- 自定义路径猜解字典
- <u>启用自定义指纹</u>

漏洞探测参数

- <u>HTTP 请求配置</u>
- 漏洞探测插件
- 其他插件配置
- 自定义弱口令配置
- 自定义路径猜解字典
- URL 去重设置



3.1.5.2 被动 Web 扫描(代理)-模板参数配置

可对 Web 站点进行漏洞扫描, 在收集扫描目标的同时, 进行漏洞检测。

- 扫描目标: Web 站点地址。
- 适用场景:需要对特定的 Web 站点资产进行更加精准的风险检测,比如:
 - 需要扫描到不容易自动爬虫到的独立页面、API 接口等信息;
 - 需要扫描到经过复杂交互,如输入特定口令才能获取的页面信息;
 - 需要根据企业业务流程,定制精准的 payload 进行测试。

基本信息

- <u>任务信息</u>
- <u>通用数据来源</u>
- <u>引擎节点选择</u>
- <u>全局白名单选择</u>

任务控制

- <u>扫描任务限制</u>
- <u>HTTP 客户端限制</u>
- 扫描白名单配置
- <u>自动生成扫描列表</u>
- 扫描动态通知
- <u>扫描结果处理方式</u>

高级扫描配置

- HTTP 请求配置
- <u>HTTPS</u> 客服端证书
- 漏洞探测插件
- 其他插件配置
- 自定义弱口令猜解字典
- <u>自定义路径猜解字典</u>
- URL 去重设置



注: 被动 Web 漏洞扫描(代理)任务创建后,使用方法和其他任务也有所不同。更多 详情,可参见下文"<u>3.1.7 代理服务器配置方法</u>"。



3.1.5.3 被动 Web 扫描(日志)-模板参数配置

可对 Web 站点进行漏洞扫描,在收集扫描目标的同时,进行漏洞检测。

- 扫描目标:日志文件中的内容。
- 适用场景:对日志文件进行解析扫描。

基本信息

- <u>任务信息</u>
- <u>日志信息采集</u>
- <u>引擎节点选择</u>
- <u>全局白名单选择</u>

任务控制

- 扫描任务限制
- HTTP 客户端限制
- 扫描白名单配置
- <u>自动生成扫描列表</u>
- 扫描动态通知
- <u>扫描结果处理方式</u>

高级扫描配置

- HTTP 请求配置
- 漏洞探测插件
- 其他插件配置
- 自定义弱口令猜解字典
- <u>自定义路径猜解字典</u>
- <u>URL 去重设置</u>

注意:要创建被动 Web 扫描(日志)任务,需要先在"系统管理/其他扫描配置/被动爬虫服务器配置"处,配置好 syslog 服务器地址。



3.1.5.4 被动 Web 扫描(镜像)-模板参数配置

该扫描策略基于 Web 的镜像流量进行扫描

- 扫描目标: 交换机上镜像的流量, 仅在硬件版上生效
- 使用场景:基于镜像流量,对 HTTP 流量进行被动收集和漏洞扫描

流量采集基础设置

- <u>任务信息</u>
- 全局白名单选择
- <u>流量信息采集</u>
- 引擎节点选择

流量采集高级设置

- <u>采集信息设置</u>
- HTTP 客户端限制
- 自动生成扫描列表
- 扫描动态通知
- <u>扫描结果处理方式</u>

流量漏洞扫描配置

- <u>HTTP 请求配置</u>
- 漏洞探测插件
- <u>其他插件配置</u>
- <u>自定义弱口令猜解字典</u>
- <u>自定义路径猜解字典</u>
- URL 去重设置



3.1.5.5 被动 Web 扫描(流量)-模版参数配置

可对 Web 站点进行漏洞扫描, 在收集扫描目标的同时, 进行漏洞检测。

- 扫描目标:流量数据中的内容。该策略在软件版上生效。
- 适用场景:对流量数据进行解析扫描。

基本信息

- <u>任务信息</u>
- 全局白名单选择
- 通用数据来源
- <u>引擎节点选择</u>

任务控制

- <u>HTTP 客户端限制</u>
- <u>扫描白名单配置</u>
- <u>自动生成扫描列表</u>
- 扫描动态通知
- 扫描结果处理方式

高级扫描配置

- HTTP 请求配置
- 漏洞探测插件
- <u>其他插件配置</u>
- 自定义弱口令猜解字典
- 自定义路径猜解字典
- URL 去重设置

注: 要创建 被动 Web 扫描(流量)任务, 需要借助流量被动扫描工具。



3.1.5.6 被动 Web 扫描 (kafka) - 模版参数配置

可对 Web 站点进行漏洞扫描, 在收集扫描目标的同时, 进行漏洞检测。

- 扫描目标: kafka 数据中的内容。
- 适用场景:对 kafka 数据进行解析扫描。

基本信息

- <u>任务信息</u>
- 全局白名单选择
- 通用数据来源
- 引擎节点选择

任务控制

- HTTP 客户端限制
- 扫描白名单配置
- 自动生成扫描列表
- 扫描动态通知
- <u>扫描结果处理方式</u>

高级扫描配置

- HTTP 请求配置
- 漏洞探测插件
- 其他插件配置
- 自定义弱口令猜解字典
- 自定义路径猜解字典
- URL 去重设置

注: 要创建 被动 Web 扫描 (kafka) 任务, 需要借助 kafka 被动扫描工具。



3.1.5.7 被动 Web 扫描 (burp) - 模板参数配置

可对 Web 站点进行漏洞扫描, 在收集扫描目标的同时, 进行漏洞检测。类似被动 Web 扫描(日志)策略。

- 扫描目标: burp 中的内容。
- 适用场景:对 burp 文件进行解析扫描。

基本信息

- 任务信息
- 全局白名单选择
- <u>目标采集</u>
- <u>引擎节点选择</u>

任务控制

- <u>HTTP 客户端限制</u>
- 扫描白名单配置
- 自动生成扫描列表
- <u>扫描动态通知</u>
- 扫描结果处理方式

高级扫描配置

- <u>HTTP 请求配置</u>
- 漏洞探测插件
- <u>其他插件配置</u>
- 自定义弱口令猜解字典
- 自定义路径猜解字典
- URL 去重设置



3.1.5.8 基础服务漏洞扫描-模板参数配置

可对服务进行基础的漏洞扫描。

- 扫描目标: 主机 IP 地址、域名。
- 适用场景:需要对特定主机上的服务进行风险检测。

基本信息

- <u>任务信息</u>
- 全局白名单选择
- <u>引擎节点选择</u>
- 扫描时间配置

任务控制

- <u>扫描任务限制</u>
- <u>扫描白名单配置</u>
- <u>自动生成扫描列表</u>
- 扫描动态通知
- <u>扫描结果处理方式</u>

信息收集参数

- <u>HTTP 请求配置</u>
- <u>主机存活探测</u>
- <u>TCP 协议扫描</u>
- UDP 协议扫描
- 其他检测选项
- <u>启用自定义指纹</u>

漏洞探测参数

- <u>HTTP 请求配置</u>
- 漏洞探测插件
- <u>其他插件配置</u>
- <u>自定义弱口令配置</u>



3.1.5.9 特定服务扫描-模板参数配置

可对指定的服务资产进行批量漏洞扫描。

- 扫描目标:端口服务。
- 适用场景:需要对特定服务进行风险检测,尤其是针对性的应急漏洞检测。

基本信息

- <u>任务信息</u>
- 全局白名单选择
- <u>引擎节点选择</u>
- 扫描时间配置

任务控制

- <u>扫描任务限制</u>
- <u>扫描白名单配置</u>
- <u>自动生成扫描列表</u>
- <u>扫描动态通知</u>
- <u>扫描结果处理方式</u>

信息收集参数

- 主机存活探测
- <u>TCP</u>协议扫描
- <u>UDP 协议扫描</u>
- 其他检测选项
- <u>启用自定义指纹</u>

漏洞探测参数

- <u>HTTP 请求配置</u>
- 漏洞探测插件
- 其他插件配置
- 自定义弱口令配置



3.1.5.10 被动服务扫描(镜像)-模板参数配置

基于镜像流量,对企业资产进行全面的收集与发现,进而对资产进行风险评估。

- 扫描目标:交换机上镜像的流量
- 适用场景:不知道自己有什么资产,需要摸清家底,并且进行风险检测,且可以提供
 镜像口的场景。

流量采集基础信息

- <u>任务信息</u>
- <u>流量信息采集</u>
- <u>引擎节点选择</u>

流量采集高级设置

- <u>采集信息设置</u>
- <u>自动生成扫描列表</u>
- 扫描动态通知
- <u>扫描结果处理方式</u>

漏洞扫描配置

- 漏洞探测插件
- 其他插件配置
- <u>自定义弱口令猜解字典</u>



3.1.5.11 主机资产监控-模板参数配置

主要对系统服务进行扫描并监控动态。

- 扫描目标: 主机 IP 地址、域名。
- 适用场景:对企业系统资产进行定期巡检,监控资产的变更和风险情况。

基本信息

- <u>任务信息</u>
- 全局白名单选择
- <u>引擎节点选择</u>
- <u>监控频率及时间设置</u>(与扫描时间设置类似,但无立即扫描)

任务控制

- 扫描任务限制
- 自动生成扫描列表
- 扫描动态通知
- <u>扫描结果处理方式</u>

监控信息设置

- <u>监控端口范围</u>
- <u>监控白名单配置</u>
- <u>监控内容设置</u>

漏洞探测参数

- 漏洞探测插件
- 其他插件配置
- 自定义弱口令猜解字典



3.1.5.12 域名资产发现-模板参数配置

可针对域名进行全面的资产发现。

- 扫描目标: 域名。
- 适用场景:需要对拥有的资产进行大面积的发现,以方便后续的风险评估和资产管理。

基本信息

- <u>任务信息</u>
- <u>引擎节点选择</u>

任务控制

- 扫描任务限制
- <u>单个扫描目标限制</u>
- DNS 解析配置
- 自动生成扫描列表
- 扫描动态通知
- <u>扫描结果处理方式</u>

高级扫描配置

- 自定义域名猜解字典
- <u>其他检测选项</u>



3.1.5.13 被动资产发现(镜像)-模板参数配置

基于镜像流量,对企业资产进行全面的收集与发现。

- 扫描目标: 交换机上镜像的流量。
- 适用场景:不知道自己有什么资产,需要摸清家底,且可以提供镜像口的场景。

流量采集基础设置

- <u>任务信息</u>
- <u>流量信息采集</u>

流量采集高级设置

- <u>采集信息设置</u>
- 自动生成扫描列表
- <u>扫描动态通知</u>
- <u>扫描结果处理方式</u>



3.1.5.14 逻辑漏洞扫描-模版参数配置

基本信息

- <u>任务信息</u>
- 全局白名单选择
- 逻辑漏洞权限配置
- 引擎节点选择

任务控制

- 扫描任务限制
- <u>HTTP 客户端限制</u>
- 扫描白名单配置
- 自动生成扫描列表
- <u>扫描动态通知</u>
- 扫描结果处理方式

高级扫描配置

- <u>HTTP 请求配置</u>
- 漏洞探测插件
- <u>其他插件配置</u>
- 自定义弱口令猜解字典
- 自定义路径猜解字典
- URL 去重设置



3.1.5.15 被动 API 扫描 (Open API)

基于 Swagger, 收集 API 信息, 对其进行漏洞扫描。

- 扫描目标: Swagger 链接或 json 文件。
- 适用场景:对 Swagger 进行解析扫描。

基本信息

- <u>任务信息</u>
- <u>信息收集</u>
- <u>全局白名单选择</u>
- <u>引擎节点选择</u>

任务控制

- <u>扫描优先级</u>
- HTTP 客户端限制
- <u>扫描白名单配置</u>
- 自动生成扫描列表
- 扫描动态通知
- 扫描结果处理方式

高级扫描配置

- HTTP 请求配置
- 漏洞探测插件
- 其他插件配置
- 自定义弱口令猜解字典
- <u>自定义路径猜解字典</u>
- <u>URL 去重设置</u>

特殊说明:

若调用接口中存在认证限制,需要在 HTTP 请求配置中增加自定义 http headers,此时请求中会带着认证进行接口调用测试



部分目标接口若存在修改数据库的情况,需要在扫描白名单配置中过滤对应的请求方式 或接口路径,以避免对生产数据造成篡改的风险

优先使用文件上传的方式,以确保扫描目标可通



3.1.6 配置参数模块

3.1.6.1 任务信息

任务信息	
◎ 扫描任务名称 ⑦	
备注	
- 扫描目标	手动输入 上传目板文件 指定资产组
	扫描目标描式:http://1.2.3.4/https://1.2.3.48000/news/?id=1http://www.chaltin.cn/
	*
* 执行类型	不走时扫描。
指定时间段 ③	通流扫描的段 值 指定禁扫时段
	起始的同 ③ 氢 低原时间 ③
	高加強定时间段

- 扫描任务名称: 1-255 个字符
 - 扫描任务名称会显示在任务列表上,也可以用于筛选;
- 备注:
 - 显示在扫描任务详情页
- 注: 被动 Web 扫描(镜像), 被动服务扫描(镜像), 被动资产扫描(镜像)不

包含以下参数项。

- 扫描目标:
 - 输入该任务需要扫描的目标
 - 手动输入:
 - ◆ 支持输入多个目标,多个目标以换行分隔。
 - 上传目标文件:
 - ◆ 支持上传单个目标文件:
 - 目标文件为.txt 格式,内容和手动输入要求相同:每行包含一个目标, 换行分隔多个目标;
 - 目标文件为 .csv 格式,用于配置批量主机登录信息,每行包含一个
 目标,以及登录方式信息。
 - ◆ 目标文件上传后,如果有异常目标,会显示异常结果的提示。包含有误的目标、出现在的上传文件的文件名、目标的行数、错误的原因。如有误, 需要修改后重新上传添加。



目标》	泰加失败,当前存在有	 	重新上传添加
4个目标有误			
有误目标	文件名	目标行数	错误原因
1.1.11	文件1.txt	10	格式校验未通过
2.2.2.2.	文件1.txt	14	格式校验未通过
http://dsfsdf	文件1.txt	25	无扫描权限
htp://dfsdf.com	文件2.txt	4	格式校验未通过
			く 1 > 10条/页>

- 指定资产组:
 - ◆ 点击"+选择资产组",打开弹窗,可以选择想要添加的资产组;
 - ◆ 可选择多个资产组。
 - ◆ 注: 被动 Web 扫描(代理), 特定服务扫描, 主机资产监控, 域名资产 扫描, 逻辑漏洞扫描不可进行指定资产组操作。
- 注: 被动 Web 扫描(日志), 被动 Web 扫描(流量), 被动 Web 扫描(kafka),
 被动 Web 扫描(burp) 不需添加扫描目标。



3.1.6.2 通用数据来源

用数据来源		
* 接收地址	请选择被动 Web 扫描(代理)接收地址	v
• 代理服务器可用端口范围 ⑦	80,443,633-890	
* 用户名		
* 肥弱		ø

- 接受地址:
 - 选择代理服务器接受地址:
 - ◆ 选择 "4.5.2.1 被动爬虫服务器配置" 配置过的内容。
- 代理服务器可用端口范围:限制任务生成代理服务的端口的范围,不填表示使用全局配置处的默认端口范围,详情请参考 4.5.2.1 被动爬虫服务器配置。
- 用户名、密码:
 - 填写地址的验证用户名和密码。



3.1.6.3 日志信息采集

这里的配置项,仅用于被动 Web 扫描(日志)这个扫描策略,对收集日志信息进行一些配置。

请选择被动 Web 扫描(日志)接收地址	
遺環写一个 Systog 服务器中可用的第口号 Systog 服务器的 IP 紀堂、信前社全局配置	船证础口可用性
请输入日志样本、每条日态以换行分周	一個的狂
	*
https->]; [请输入目态文件的主机 IP 或域名	; 調口 🗹 日志内 host 优先
	通送得被劲 Web 扫描(日志)模收地址 帶填写一个 50% 國務最中可用的第口号 Systog 國務務的 P 配置。请前往全局配置 请输入日志祥本、每条日志以供行分類 Mtps√」: 请输入日志文件的主机 P 或域名

● 接受地址:

■ 选择代理服务器接受地址:

◆ 选择 "4.5.2.1 被动爬虫服务器配置"配置过的内容。

- Syslog 服务器连接配置:
 - Syslog 服务器 IP , 点击 "全局配置", 前往全局页面进行配置;
 - Syslog 服务器端口,填写通信的端口数字,填写完后可以点击右侧的"验证端 口可用性"进行验证,给出可用的提示信息,即可正常使用。
- 日志参数匹配规则:
 - 选取解析日志的规则;
 - 点击下拉菜单选择规则。
- 验证日志规则有效性:
 - 输入要解析的日志样例,验证规则是否可以正常解析。
- host 设置:
 - 对于日志文件中没有 host 信息的, 可以在此处配置:
 - ◆ 选择协议,填写服务器 IP 和端口。

传输日志数据方法说明



下载"日志传输客户端"辅助工具(联系公司内部技术支持人员获取)。当前工具版本:洞鉴(X-Ray)辅助工具-日志传输客户端 v6

● 客户端适用系统说明

工具名称	适用系统
pioneer_darwin_amd64	MAC 64 位
pioneer_darwin_386	MAC 32 位
pioneer_linux_amd64	Linux 64 位
pioneer_linux_386	Linux 32 位
pioneer_windows_386	Windows 32 位
pioneer_windows_amd64	Windows 64 位

● 工具使用说明:

■ 操作指令: [工具名称] send-log-file --log-server-host [洞鉴部署的服务器

IP] --log-server-port [传输日志的端口] --logfile [日志文件名逗号分隔]

--log-per-second [数字, 建议 10] --disable-filter

mac 样例: ./pioneer_darwin_amd64 send-log-file --log-server-host

192.168.54.17 -- log-server-port 1234 -- logfile ../users.log -- log-per-

second 10 -- disable-filter

● mac 下使用样例:

→ 洞鉴**(X-Ray)辅助工具-日志传输客户端v4** ./pioneer_darwin_amd64 send-log-file --log-server-host 192.16 er-port 1234 --logfile ../users.log --log-per-second 10 [INFO] 2020-04-08 13:07:26 +0800 [default:log.go:159] 待传输的的日志文件为: ../users.log [INFO] 2020-04-08 13:07:26 +0800 [default:log.go:159] 当前配置的RPC服务器地址为: 127.0.0.1:15832 [INFO] 2020-04-08 13:07:26 +0800 [default:log.go:159] 开始传输日志: ../users.log



3.1.6.4 流量信息采集

此处主要用于采集<mark>镜像</mark>流量,适用于洞鉴硬件版。软件版流量采集参数配置说明见 通用数据来源。

* 接收地址	请选择被动 Web 扫描(镜像)接收地址	~
•选择流量网卡		

- 接受地址:
 - 选择代理服务器接受地址:
 - ◆ 选择 "<u>4.5.2.1 被动爬虫服务器配置</u>"配置过的内容。
- 选择流量网卡:
 - 具体网口配置请参考 4.1.3.2 网口配置。

此处主要用于流量或 kafka 被动扫描。

通用数据来源			
		流量被动扫描任务需先下载 <mark>软件版流量被动扫描工具</mark> 。根据工具包中的使用说明 配置 通用数据转发	
	*接收地址 ③	请选择通用数据读母地址	v r
通用数据来源			
		kafka 被动扫描任务需先下载kafka 被动扫描工具,根据工具包中的使用说明配置通用数据转发	
		德治國議師教師國政(444)	

- 接收地址
 - 选择通用数据接收地址 IP, 接收地址列表为管理节点可访问的引擎节点地址;
 - 填写通用数据接收地址 IP,根据机器的端口开放情况和自身需要,填写任务占用的端口。

通用数据接收方法说明:

- 下载 "kafka 被动扫描工具"或 "流量被动扫描工具";
- 根据工具包中的说明文档,启动被动 web 扫描客户端;


- 工具使用注意事项:
 - 先创建任务后,再进行 流量/kafka 被动扫描工具配置,以避免操作客户端工
 具时,没有数据接收端口。



3.1.6.5 目标采集

这里的配置项,仅用于被动 Web 扫描(burp)这个扫描策略,对上传的 burp 信息 进行采集。

标米集			
	* burp文件		
		点击或将文件拖拽到这里上传	
		文件大小不超过 100 M;文件类型:.xml	

支持上传不超过 100M 的文件, 文件格式为".xml"



3.1.6.6 信息收集

这里的配置项,仅用于被动 API 扫描(Open API)这个扫描策略,对目标信息进行采集。

信息收集					
		播政地址 文件上傳			
	* 接收地址	课编写可用于被动扫描就即想意约 Bwogger 图绘			
自意收集					
愿收集		接攻地址 文符上传			
1.8收集	* Swagger (HB	接收地址 文伟上传			
意改集	* Swagger (F.D.	接收地址 文帝上传	j		



3.1.6.7 逻辑漏洞权限配置

用于配置不同权限的账号 cookie,用于检查越权漏洞。

逻辑漏洞权限配置				
* 被源帐号 Cookie ⑦	cooldo 认证的词	请输入用于测试的 Cooke 监号	1	¥.
	+ 琥如一番用户认证信息			

- 被测账号 Cookie:
 - 代理访问的用户默认为权限最高用户账号,此处填写的账号默认为低权限用
 户,且等级数字越小,权限越高。
 - 对应填写的信息:
 - ◆ Cookie 认证的域:支持输入 IP 或域名;
 - ◆ Cookie 值:Cookie 认证的域对应的 Cookie 值;
 - ◆ 权限等级:数字越小,权限越大,默认选中1。
- 添加一条用户认证信息:
 - 支持添加更多权限不同的账户信息。



3.1.6.8 引擎节点选择

显示当前系统部署的所有引擎节点,默认选中一个引擎节点,用户可按需选择同时 启动的节点。

- 单选:
 - 只能选择一个引擎节点;
 - 仅适用于:基础 Web 漏洞扫描,逻辑漏洞扫描



● 多选:

■ 能选择多个引擎节点,任务目标会被分配到不同节点进行扫描;

引擎启用	引擎节点 IP	引擎名称	标签	引擎状态	可用组织单位	
	169.254.1.1	testaaa		空闲	默认工作区	
						< 1 → 10条/页∨



3.1.6.9 扫描优先级

扫描优先级	可以选择定义该任务期 级,系统将优先调度周	可以选择定义该任务期望的执行优先 级,系统将优先调度高优先级的任务			
	•任务扫描优先级 ⑦	紧急	高	中	低

- 任务扫描优先级:
 - 可以配置该项目决定在引擎资源饱和后的优先级调度,优先级越高的任务在有 引擎资源是释放后越能优先被调度
 - 适用于所有策略



3.1.6.10 扫描任务限制

扫描任务限制		
*任务最大运行时间	180	分钟
* 允许收集的最大链接数 ⑦	10000	

- 任务最大运行时间:
 - 限制任务执行的最大时间,默认为3小时。
 - 当任务总执行时间超过此限制时,将强制结束任务。
- 允许收集的最大链接数:
 - 限制该任务扫描时收集的最大链接数量。
 - 任务收集的链接超过该数量后,不会再继续收集链接。

仅应用于以下参数的扫描策略:基础服务漏洞扫描,特定服务扫描。

扫描任务限制		
•任务最大运行时间 ⑦	180	分钟
* 最大并发主机数	50	
* 最大带宽占用限制 ⑦	2000	KB/s
	新能流量管控	

- 任务最大运行时间:
 - 限制任务执行的最大时间,默认为3小时。
 - 当任务总执行时间超过此限制时,将强制结束任务。
- 最大并发主机:
 - 主机扫描可同时执行的主机数,最大并发主机数越高,扫描速度越快,性能消耗越强。
- 最大带宽限制:
 - 主机扫描任务全局带宽限制,可控制主机扫描的信息收集以及漏洞扫描阶段, 引擎消耗的最大带宽。
 - 单位是 KB/s。
 - 智能流量管控:
 - ◆ 由引擎智能根据当前请求的返回情况调节扫描速度,以最优的资源占用实现高效扫描



3.1.6.11 HTTP 客户端限制

HTTP 客户端限制		
*请求失败后的重试次数 ③	1	
* 最大重定向次数 ③	5	
- HTTP 请求连接超时时间 ③	3000	進む
- HTTP 请求喻应超时时间⑦	10000	花 砂
*每个站点并发连接数 ⑦	50	
•每秒最大请求数 ③	500	
。页面大小限制 ③	10240	КВ

- 请求失败后的重试次数:
 - 设置对扫描目标发送 HTTP 请求失败后,最大的重试次数;
 - 若重试过该次数后,仍然请求失败,任务就不会再尝试对该目标发送请求;
 - 设置合适的请求重试次数,和下文中的"HTTP请求连接超时时间"、"HTTP

请求响应超时时间"相配合,可以最大程度地降低网络波动等意外情况对任务 扫描过程的影响,同时保证任务扫描的效率。

- 最大重定向次数:
 - 限制一次 HTTP 请求重定向的次数;
 - 任务对目标发送一次 HTTP 请求时,遇到 30X 重定向的次数超过最大重定 向次数时,任务就不会再继续跟随;
 - 如果目标重定向次数过多,甚至无限递归,任务无限制地跟随会耗费大量资源;
 - 适当限制最大重定向次数可以减少这个问题造成的影响,同时能够正常收集使 用重定向的目标的信息。
- HTTP 请求连接超时时间(单位为毫秒):
 - 限制任务发送 HTTP 请求进行 TCP 连接的超时时间;
 - 若超过该时间仍未连接,则判断为连接超时,请求失败;
 - HTTP 请求连接时间过长的原因可能是网络未连接、参数错误、缺少证书等, 此时任务继续等待也无法连接,只会不断耗费时间;
 - 适当限制连接超时时间有助于避免这种情况。
- HTTP 请求响应超时时间(单位为毫秒):



- 限制任务发送 HTTP 请求后等待响应的最大时间;
- 若超过该时间未得到目标的响应,则判断为响应超时,请求失败;
- HTTP 请求长时间未响应可能是因为服务器忙碌、防火墙拦截等,尤其是防火 墙拦截即使继续等待也不会得到响应;
- 适当限制响应超时时间,有助于避免因为这种情况耗费太多时间。
- 每个站点并发连接数:
 - 限制任务在扫描过程中允许并发连接的最大数量;
 - 任务在扫描过程中同时连接多个目标尝试扫描,可以提高扫描的速度,但也会 占用服务器的运行资源;
 - 适当限制并发连接数,能在服务器处理能力内最大程度地低提高扫描的速度。
- 每秒最大请求数:
 - 限制该任务扫描时,每秒能发送的最大请求数;
 - 每秒请求数量太低会对扫描速度产生影响,但太高会占用洞鉴服务器的运行资源,也有可能对扫描目标服务器造成负担;
 - 适当限制每秒请求数量,可以尽可能地在不造成负面影响的情况下提升扫描速度。
- 页面大小限制(单位为 KB):
 - 限制读取单个页面的 HTTP 响应时的页面大小;
 - 若超过页面大小限制,则不会再继续读取超过限制的部分;
 - 单个页面太大的话,任务不加限制的读取扫描将会耗费很多的资源和时间;
 - 在了解需扫描目标的页面大小的情况下,适当限制读取页面的大小,有时能够 很大程度地节约扫描的时间。



3.1.6.12 扫描白名单配置

该模块默认开启。开启后,排除扫描目标中不进行漏洞检测或者不进行资产发现的 目标。

主机白名单配置:

扫描白名单配置	
白名単应用 ⑦	v)
規避扫描的主机目标 ⑦	白名早格式,回车换行分漏 www.website.com *.website.com 1.1.1.1 1.1.1.0-255 1.1.1.1724 [234-0] 1.1.1.190
扫描白名单适用 ⑦	✓ 不进行资产发现 ☑ 不进行漏漏检测

Web 白名单配置:

扫描白名单配置		(启用)
白名单应用 ⑦		×
规避扫描的 Web 目标 ⑦	白名单格式。回车换行分隔 http://www.website.com/ https://www.website.com/admin+ https://www.website.com/admin+ 若目标白名单为类似 http://dwwa.vul.ct:9020/7id=1&Submit=Submit 的形式,请不要省略??后的内容,或者用 http://dwwa.	.vul.et:9020/* 代譜
扫描白名单适用 ⑦	不进行资产发现 还 不进行温润检测	

- 白名单应用:可以选择全局白名单中预置好的白名单模版,进行编辑填充
- 规避扫描的目标:
 - 按照格式要求,手动填写不想进行漏洞检测或不想进行资产发现的目标地址;
 - ◆ 主机白名单支持 IP 段、IP 加端口的格式,详细见 placeholder。
- 扫描白名单适用范围可以多选:
 - 不进行资产发现:不进行资产发现与漏洞检测
 - 不进行漏洞探测:进行资产发现,但是不进行漏洞检测
- 不扫描包含以下关键字的 URL(Web 策略)
 - 限制任务爬虫爬取的范围;

- 配置后,任务在爬取链接过程中,若判断出 URL 中包含指定的关键字,就会 主动停止该次访问;
- 配置合适的关键字,如 delete、remove、logout 等来排除 URL,有助于减 小爬虫对资源破坏的几率、也有利于爬虫信息收集的完整性。
- 具体配置方法为:
 - ◆ 输入需要排除的关键字,按回车键添加;
 - ◆ 点击关键字右侧的关闭图标,可以删除已添加的关键字。



3.1.6.13 采集信息设置

主要用于对镜像流量的采集和筛选。

采集信息设置	
主动识别指纹	
収集流量范围 ③	请输入要收集的 IP 地址范围,为空表示不健雅制,回车执行分隔:1,1.1.11,1.1.1241,1.1.1.255
	· 请输入墨收集的端口范围。为空表示不做限制。英文道号分隔:1,100,300-1000
不收集流量范围 ③	#输入要收集的 IP 地址范围,为空表示不做理制,回车执行分隔:1.1.1.11.1.1.1/241.1.1.1.265
	10000-65535

- 主动识别指纹:
 - 默认开启,开启后会对采集的流量进行主动探测指纹。
 - 关闭后,不再对指纹进行主动探测,流量中采集到的是什么信息就是什么信息。
- 收集流量范围:
 - 可以对要采集流量的 IP 和端口进行限制;
 - 不设置,表示所有端口都会捕获;
 - 设置后,只收集地址为设置 IP 和端口的流量。
- 不收集流量范围:
 - 可以对不采集流量的 IP 和端口进行限制;
 - 不设置,表示所有端口都会捕获;
 - 设置后,填写的 IP 和端口相关的流量均不会收集。



3.1.6.14 单个扫描目标限制

单个扫描目标限制		
*单个目标最大扫描时间 ⑦	10	分钟
* 最大子域名深度 ⑦	5	
* 并发 DNS 查询数量 ⑦	80	

- 单个目标最大扫描时间:
 - 限制每个目标的最大扫描时间。超过限制时,会直接结束对当前目标的扫描。
 - 如果任务目标较多,限制单个目标最大扫描时间可以有效的控制任务的总时 长,避免网络波动、网站防御等情况对任务效率造成过大的影响。不过单个目 标最大扫描时间太短,可能还没收集到什么信息,就结束该目标的扫描了。通 常情况下,如果任务目标只有几个,则建议把单个目标最大扫描时间设高一些, 以避免信息收集和漏洞探测不全
- 最大子域名深度:
 - 限制任务递归猜解的最大子域名深度。超过了此限制后,就不会继续猜解。
 - 任务在进行目标的域名发现时,会自动猜解子域名,猜解成功后默认会继续递 归猜解。一般情况下,三、四级子域名就算是比较多的了。但是一些特殊设计 的域名结构或 DNS 服务器规则,可能对目标的所有子域名都返回 IP 结果, 导致无限制的递归猜解。为了避免这种情况,就需要限制最大子域名深度。设 置的时候参考实际的域名级数,不要设得太小以免域名发现不全就可以了。
- 并发 DNS 查询数量:
 - 限制任务同时发送 DNS 请求的线程的最大数量。
 - DNS 查询可以用于发现域名资产,解析域名 IP 等。如果并发 DNS 查询数

量太大, 容易给 DNS 服务器造成压力;反之, 并发 DNS 查询数量太小则 可 能影响扫描速度 。



3.1.6.15 DNS 解析配置

此处用以配置全局 DNS 配置无法解析的扫描目标。

DNS 解析配置	(III)
* DNS 服务器	服务器搭式, 以回年执行分期: 1.1.1.12.2.2.2

- 此配置项默认处于关闭状态。
- 开启后,按要求格式填写 IP 地址,换行分隔:
 - 当前填写的 IP 地址会覆盖全局配置的 DNS 配置。



3.1.6.16 自动生成扫描列表

开启后,任务在每次扫描结束后将自动生成报告,可前往报告管理下载。如果开启 了扫描动态通知,选中的不同格式的扫描报表会自动发送至邮箱。

 如果资产组开启了"任务发送报表通知",则会将选中格式的报表文件发送至资产组 绑定邮箱。

自动生成扫描报表					
	*模板名称 ⑨	扫描任务报表模板			v
	*报表文件格式	Word& Excelle VITALIS PDF&			

- 报表名称:
 - 默认为自定义的扫描任务报表模版,也可以选择自定义的模板或英文模版。
- 报表文件格式:
 - 系统默认选择 HTML 版
 - 用户可自行选择 Word 版, Excel 版, PDF 版。

3.1.6.17 扫描动态通知

启用时,每次任务结束后系统都将自动给此处填写的邮箱发送邮件通知。对于扫描 耗时较长、或是定时扫描的任务,开启扫描动态通知,可以在收到邮件通知后再查看扫 描结果,而不需要频繁查看任务以获得扫描结果。

扫描动态通知			
	*接受通知的邮箱 ⑦	多个都箱地址之间可以换行分期,邮箱格式如下: alarm@example.comreport@cooc.com	
		清输入正确的邮箱地址	h

- 接收通知的邮箱:
 - 在此填写需要接收通知的邮箱;
 - 支持同时输入多个邮箱,多个邮箱以换行分隔。
 - 邮箱格式如下:
 - ◆ alarm@example.com
 - report@xxxx.com
 - 注意:只有在系统 SMTP 配置成功的情况下,邮箱才能够接收到通知。关于

SMTP 配置的详细信息可参见 4.1.1.3 SMTP 服务器设置。



3.1.6.18 扫描结果处理方式

对扫描结果的处理方式做自定义的配置

扫描结果处理方式	
将结果更新到资产管理	
同步创建资产	
将结果更新到漏洞管理	
自动标记已修复漏洞 ③ 🤇	
自动生成完整扫描日志(

- 将结果更新到资产管理:
 - 默认开启,扫描结果中的资产信息将自动更新到资产中心;
 - 结果更新的前提是创建了该资产,该资产存在才可以将结果更新到资产中,否则什么都不做;
 - 关于资产分配:
 - 服务资产更新到主机资产详情中端口列表;
 - ◆ 域名资产更新到 web 资产详情中目录结构信息。
- 同步创建资产:
 - 默认开启,
- 将结果更新到漏洞管理:
 - 默认开启,扫描结果中的漏洞信息将自动更新到漏洞管理;
 - 若漏洞管理中不存在,任务会将其自动添加到漏洞管理中;
 - 若漏洞管理中以存在:
 - ◆ 且漏洞状态为"已修复",任务会以"未分配"状态更新该漏洞;
 - ◆ 且漏洞状态不为"已修复",则漏洞管理中的状态不会被改变。
- 自动标记已修复漏洞:
 - 默认关闭,开启后,某目标下已存在的漏洞,若在本次扫描中未被发现,会自动置为已修复状态。"忽略"以及"误报"状态的漏洞除外。
- 自动生成完整扫描日志:
 - 默认关闭,开启后在扫描日志中会生成 debug 日志,便于定位扫描过程中遇 到的问题。



3.1.6.19 HTTP 请求配置

对任务在信息收集阶段或漏洞探测阶段发送的 HTTP 请求做详细配置。

HTTP 请求配置	
* User-Agent	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36
Cookie 🗇	uid_example=12345; Finger-abc; session=ABC
	> 廣极這项
其他自定义 HTTP 请求头 ③	+ 環加一个新的自定义 HTTP 请求头
の 現分 91714	英诗配置多个代理,换行分强,舆: http://1.2.3.4.1080/ https://1.2.3.4.1080/ socks5//1.2.3.4.1080/
	清输入正确的 HTTP 代理 必

- User-Agent:
 - 配置后,任务将使用这里的 User-Agent 作为请求头发送请求;
 - 某些目标对特定 User-Agent 的请求访问有所限制,配置合适的 User-Agent 可以解决这个问题。
 - 配置的具体方法有两种:
 - ◆ 直接输入所需 User-Agent 的值;
 - ◆ 点击 User-Agent 输入框, 在下拉备选菜单中点击需要配置的值。
- Cookie:
 - 配置后,任务将使用这里的 Cookie 作为请求头发送请求;
 - 配置好正确的 Cookie 后,才可以扫描某些需要 Cookie 认证的目标,
 - 配置时,可以对每个 Cookie 选择是否 "允许覆盖";
 - ◆ 若不允许覆盖,任务会始终使用该 Cookie 配置的值;
 - ◆ 否则,任务会根据返回信息重新设置 Cookie,更符合真实访问情况。

- 如果服务器对该 Cookie 的访问限制是相对不变的,选择不允许覆盖该
 Cookie,可以保证扫描信息与预期一致,也能有效地避免爬虫时自动登出的问题;
- ◆ 如果服务器对该 Cookie 的访问限制是动态的、需要实时更新才能保持登
 陆,又或者是需要扫描的漏洞与 Cookie 覆盖行为本身相关,那么允许覆
 盖该 Cookie 才能更真实地获取目标信息。
- 配置的具体方法为:
 - ◆ 直接输入 Cookie 内容, 样例如上图中所示;
 - ◆ 展开"高级选项",可以预览配置的 Cookie 信息,并且可以对每一条
 Cookie 选择是否"允许覆盖"。
- 逻辑漏洞扫描不需要配置 Cookie
- 其他自定义 HTTP 请求头:
 - 配置后,任务将使用这里的 HTTP 请求头发送请求;
 - 配置特定的请求头,可以应对扫描目标可能存在的、对访问的特殊限制。
 - 配置的具体方法为:
 - ◆ 点击"+ 增加一个 HTTP 请求头",填写请求头的名称与值;
 - ◆ 可以同时添加多条自定义 HTTP 请求头;
 - ◆ 点击已添加 HTTP 请求头的删除图标,可以删除该 HTTP 请求头。
- HTTP 代理:
 - 填写后,任务将使用此 HTTP 代理来扫描目标;
 - 如果洞鉴服务器因为某些原因(如和目标不在同一个网络、目标对访问者 IP 有 所限制等)无法直接访问需要扫描的目标,配置合适的 HTTP 代理可以解决 问题配置的具体方法为:



- ◆ 直接输入 HTTP 代理的 URL;
- ◆ 注意:配置时代理时请确保洞鉴服务器可以访问到该 HTTP 代理,且该HTTP 代理可以访问到扫描目标
- 支持配置多个代理,通过换行符分隔



3.1.6.20 HTTPS 客服端证书

默认关闭, HTTPS 客户端证书启用且配置正确后, 可以扫描某些需要 HTTPS 客户端证书认证的目标。

HTTPS 客户端证书 ⑦	e	D
* HTTPS 客户端证书文件	点击或将文件拖拽到这里上传 文件大小不超过 10 M	
HTTPS 客户端证书密码	请输入正确的客户端证书女件	
	请输入证确的客户端证书密码	



3.1.6.21 HTTP 基础认证

默认关闭, HTTP 基础认证启用且配置正确后,才可以扫描某些需要 HTTP 基础 认证的目标。

HTTP 基础认证	
用户名	
密码	

● 用户名:

- 填写 HTTP 基础认证的用户名;
- 若启用 HTTP 基础认证但不填写用户名,任务将使用空用户名尝试认证。
- 密码:
 - 填写 HTTP 基础认证的密码;
 - 若启用 HTTP 基础认证但不填写密码,任务将使用空密码尝试认证。



3.1.6.22 Web 表单登录

默认关闭, Web 表单登录启用且配置正确后, 才可以扫描某些需要表单登录的目标。

Web 表单登录	
* 表单所在的 URL	
	请输入正确的 URL
用户名	
密码	

● 表单所在的 URL:

- 填写进行表单登录的 URL;
- 用户名:
 - 填写表单登录的用户名;
 - 若启用 Web 表单登录但不填写用户名,任务将使用空用户名尝试登录。
- 密码:
 - 填写表单登录的密码;
 - 若启用 Web 表单登录但不填写密码,任务将使用空密码尝试登录。

3.1.6.23 网站可用性验证

默认关闭, 启用后任务在扫描 Web 站点之前, 会先对网站进行可用性验证, 确认 网站可用再进行扫描, 否则任务将不考虑网站的存活情况, 直接尝试扫描。

由于直接扫描不存活的网站一般耗时较久, 启用并合理配置网站可用性验证, 可以提高扫描的速度。

网站可用性验证		SHI)
	* 验证地址 ①	
	* 特征字符串	-462

● 验证地址:

- 填写可以验证网站可用性的地址。
- 特征字符串:
 - 填写网站的 response 字段,点击"一键验证",验证网站是否可达;
 - 如果失败,说明网站不可达。

3.1.6.24 Web 爬虫

默认开启,任务会使用 Web 爬虫以收集网站的更多信息;若关闭 Web 爬虫,任 务将只扫描用户填写的目标网站。

启用并合理配置 Web 爬虫,可以收集更多关于网站的信息,而不仅局限于填写的目标。

Web 爬虫		
模拟真实浏览器渲染页面 ③		
允许爬取父目录		
允许的 HTTP 请求方式	GET × HEAD × POST × PUT × OPTIONS ×	
最大龍取深度 ⑦	● 请输入正确的最大质取深度	
允许爬取的域 ⑦		
不爬取包含以下关键字的 URL ③	delete × remove × logout ×	

- 模拟真实浏览器渲染页面:
 - 默认关闭

■ 开启后爬虫会模拟浏览器的行为来解析 HTML 页面,并执行其中的

JavaScript 脚本;

Web 爬虫		
權拟真实浏览器渲染页面 ③		
登录序列文件 ③	上 上传文件 支持下最登录录制工具。使用"登录录制工具"可录制用户在波览器的操作,上传生成的yami可在扫描时自动重数登录操作	
探索序列文件	<u>よ 上传文件</u> 文件格式为 yami; 使用此功能需要 iconse 包含 "板边 Web 扫描(Ixup)" 扫描 集構	
允许能取父目录		
允许的 HTTP 请求方式	GET × HEAD × POST × PUT × OPTIONS ×	
最大應取得度 ①	5	
允许源取的城 ③		

■ 否则爬虫只会使用普通的 HTML 解析器来解析页面中的表单与链接。



- 若网页的前端代码中使用了大量的 JavaScript 脚本来实现页面, 启用该选项 可以更加真实地收集页面的信息;
- 但模拟浏览器渲染页面比较耗时,会降低任务的扫描速度。
- 允许爬取父目录
 - 默认关闭,开启后任务会尝试爬取扫描目标的父目录,否则只会爬取目标和目标的子目录;
 - 爬取父目录可以收集到更多的页面信息,但会增加任务的耗时。
- 允许的 HTTP 请求方式:
 - 限制任务扫描时允许使用的 HTTP 请求方式;
 - 任务将只使用此处填写的方式来发送请求。
 - 注意:不当的请求方式有可能造成目标资源的损坏,如 DELETE、PUT、

POST, 请谨慎使用此类请求方式。

- 具体配置方法为:
 - ◆ 输入允许的 HTTP 请求方式, 按回车键添加;
 - ◆ 或是点击输入框,在下拉菜单中点击需要的请求方式,
 - ◆ 系统可以使用的请求方式有:GET、POST、PUT、HEAD、 OPTIONS、

DELETE, TRACE, CONNECT;

- ◆ 点击请求方式右侧的关闭图标,可以删除已添加的请求方式。
- 最大爬取深度:
 - 限制任务爬虫时最大的爬取深度;
 - 当任务将单个目标设为起始页,一层层追踪链接,层数达到最大爬取深度时, 就会停止向下追踪;
 - 爬取深度更大时,任务可能收集到更多的信息,但也会增加任务的耗时;
 - 适当限制最大爬取深度,可以让任务在能够接受的耗时内最大程度收集信息。
- 允许爬取的域
 - 限制任务爬虫爬取的范围;
 - 配置后,任务会额外爬取允许爬取的域,否则任务将只爬取和扫描目标中 URL 相同的域。
 - 添加允许爬取的域,可以扩大任务信息收集的广度;
 - 用户可以根据实际所需配置,如允许任务爬取一些子域,这些子域和扫描目标

中的 URL 相同。

- 具体配置方法为:
 - 输入允许爬取的域,按回车键添加;



- ◆ 系统支持通配符 "*", 如可以使用 "* .test.com"、" *.test.cn" 等;
- ◆ 点击域右侧的关闭图标,可以删除已添加的域。



3.1.6.25 主机存活探测

启用后,任务执行时,会先执行一次快速预扫描,发现扫描目标中存活的主机。

由于直接扫描不存活的主机,无效且费时,启用并恰当配置主机存活探测,能够大幅提升任务扫描的速度。

主机存活探测 ⑦		(BR)
•探测方式	ICMP	
- 探测强度	快速探測 常規探測 純准探測 自定义探测	
超时等待时长		Ð
最小重试次数		次
最大重试次数		次
跳过不存活主机 ⊙	0	

- 探测方式:
 - 点击下拉菜单选择方式。
- 探测强度:
 - 选择主机探测的强度;
 - 用户可以根据对扫描速度和精度的需求自行选择。
- 超时等待时长:
 - 固定为1秒。
- 最小重试次数:
 - 固定为3次。
- 最大重试次数:
 - 固定为100次。
- 跳过无响应的主机
 - 启用后,对于主机存活探测中发现不存活的主机,任务不会再尝试扫描;
 - 否则任务会不考虑主机存活状态,直接尝试扫描所有主机。
 - 关闭时可能导致扫描速度大幅下降。



3.1.6.26 TCP 扫描协议

启用后,可以对任务扫描的 TCP 端口进行自定义。关闭时,任务会使用默认的端口组扫描目标。启用并配置后如下图所示:

TCP 协议扫描		金用
* 端口列表 ⑦	7,9,13,21-23,25-26,37,53,79-81,88,106,110-111,113,119,135,139,145-144,179,199,389,427,443-445,465,513-615,543- 544,546,554,567,631,646,873,886,990,993,995,1025-1029,1080,1110,1433,1443,1720,1723,1755,1900,2000- 2001,2049,2121,2181,2717,3000,3128,3396,3389,3886,4899,5000,5009,5051,5060,5101,5190,5357,5432,5631,5666,5800,5800,6000- 6001,8646,7000-7005,7070,8000,8008-8009,8080-8081,8443,8886,9100,9999-10000,11211,32766,49152-49157	+ 导入罐口组
	译输入正确的 TCP 端口	
* 扫描方式 ③	SYN	
* 扫描强度	快速探测 常规探测 精准探测 自定义探测	
超时等待时长		秒
最小重试次数		次
最大重试次数		次
指纹探测 ⑦		
探測精度	性構成探測 机机工工 高精度探测	

- 端口列表:
 - 输入需要扫描的 TCP 端口;
 - 具体配置方法:
 - ◆ 直接输入端口;
 - 输入端口号,多个端口号之间以英文逗号","分隔;
 - 支持输入端口段,如:"10-18"。
 - ◆ 导入端口组:
 - 点击"+导入端口组";
 - 在弹窗中选中要导入的端口组,点击"确定";
 - 端口组中的端口会自动加入当前的端口列表后方。
 - 特定服务扫描不需要输入端口。
- 扫描方式:
 - 选择对 TCP 端口对扫描方式;
 - TCP CONNECT 方式结果准确,但速度较慢;



- TCP SYN 方式速度较快,但有一定误差;
- 用户可根据对扫描速度和精度的需求自行选择。
- 扫描前度:
 - 基于不同的扫描强度会加载不同的参数配置;
 - 强度分为快速扫描、常规扫描、精准扫描和自定义扫描。
 - ◆ 其中扫描速度快速扫描>常规扫描>精准扫描;
 - ◆ 扫描精准度精准扫描>常规扫描>快速扫描;
 - ◆ 在以上选项时参数不可配,需要调整参数则要选择自定义选项。
- TCP SYN 可控参数
 - 超时等待时长,控制连接的超时时长限定
 - 最小重试次数,控制连接不成功时重试的最小次数
 - 最大重试次数,控制连接不成功时重试的最大次数
- TCP Connect 可控参数
 - 超时等待时长,控制连接的超时时长限定
 - 最大并发端口连接数,控制同时并发的端口数
 - 最大 QPS, 限制每秒最大请求数
- 指纹探测:
 - 启用指纹探测时,任务会尝试探测发现的开放端口上的服务和应用。
 - 启用后,可更改探测精度:
 - ◆ 低, 中, 高



3.1.6.27 主机登录扫描

默认不开启, 启用后, 可以对扫描目标中输入的主机资产进行主机登录扫描。点击 选择目标进行主机选择

<·〉 洞鉴 _x -						
默认工作区	▶ 1理	/ 任务列表 / 編輯扫描任务	5			
◎ 全局仪表盘		选择目标主机			×	
⊖ 扫描管理	^ ±		资产地址			
扫描策略			10.9.33.39			
任务列表			10.9.33.122		登录端口	用户名
扫描设置	~		10.9.33.123			
▲ 基线管理	*			< 1 > 10条/页		
意 资产中心	~				_	
☆ 漏洞管理	•			ā	定	
自 报表中心	*					
🖸 知识牌	~				保存任务 保	存并立即扫描

选择主机资产后,进行用户名密码的配置。输入主机用户名以及登录所使用的密码或者私钥,点击登录验证。成功后,点击确定即配置该主机成功。

<→ 洞鉴 x						
默认工作区	×					
① 全局仪表盘			主机登录设置	×		
8 扫描管理	*		* 登录协议	SSH 🗸		CR.M.O
任务统计 归植策略	检测	目标 选择目	*服务端口	22		清空已选目标
任务判决	1		* 用户名	请输入该主机可用的登录用户名	用户名	操作
扫描设置	.*.		*认证口令	密码 私钥	22.	KATSH MICH
⊿ 基线管理	*					MAN BIRK
● 资产中心	*		*密码	请输入该主机可用的登录密码		MATH BIRS
血 漏洞管理	~			登录验证	< 1	⇒ 10 条/页 ∨
圖 报表中心	.*					
〇 知识库	~			取消 确定	保存任务	保存并立即扫描
C 2 40 00 10						



同鉴x			◎ 登录验证成功		
۲X	V				
义表盘		主机登录设置		×	
理	*	* 登录协议	SSH	-	(BA
统计	检测目标 选择目	*服务端口	22		清空已选目标
東略	1 0	* 用户名	root	用户名	操作
9 2	•	* 认证口令	100.7.7. <u>新</u> , 4日	-	编辑 删除
印理	• 🗆	MILLIY	נבו אש אדער אין	•	编辑 删除
1 (Č).	• 🗆	*密码		•	编辑 删除
躍	*		登录验证	< 1	> 10 条/页 →
NDA	*				
	*		取消确定	定 保存任	务保存并立即扫描

也可对主机进行批量配置用户名密码后登录验证。



3.1.6.28 UDP 端口扫描

启用后,可以对任务扫描的 UDP 端口进行自定义;关闭时,任务不会扫描 UDP 端口。

UDP 协议扫描 ⑦		出用
* 扫描方式	UDP 风能器器:蛋白白癌程序通常未适分附打开的和已过虚约UDP端口之间的反射。应用UDP端口扫描程序可能会大大规划扫描时间并产生不可重的感觉。	
- 端口利表 ③	+ 95218[24]	
* 扫描强度	第論人正确的 UDP 第回	
超时等待时长		Ð
最小重试次数		次
最大重试次数		次

注: UDP 端口扫描速度较慢, 且结果误差大, 在没有强烈需求的情况下建议关闭。

- 端口列表:
 - 输入需要扫描的 UDP 端口;
 - 具体配置方法为:
 - ◆ 直接输入端口:
 - 输入端口号,多个端口号之间以英文逗号","分隔;
 - 支持输入端口段, 如"10-18"。
 - ◆ 导入端口组
 - 点击"+导入端口组";
 - 在弹窗中选中要导入的端口组,点击"确定";
 - 端口组中的端口会自动加入当前的端口列表的后方。
 - 特定服务扫描不需要输入端口。
- 扫描强度:
 - 仅提供常规扫描;
- 超时等待时长:控制连接的超时时长限定;
- 最小重试次数:控制连接不成功时重试的最小次数;
- 最大重试次数:控制连接不成功时重试的最大次数。



3.1.6.29 其他检测选项

其他检测选项	
是否启用局域网加速 ③ 💽	
是否对 IP 进行域名反解 ③	

- 是否启用局域网加速:
 - 如果扫描目标和扫描器处于同一局域网中,那么使用 APP 来优化扫描请求。
- 是否对 IP 进行域名反解:
 - 通过 DNS 反解查询扫描结果中 IP 对应的域名。



3.1.6.30 启用自定义指纹

启用后,同类指纹以自定义为准。

启用自定义指纹 ①						
	0項	已启用的扫描插件		0项	未启用的扫描插件	
	请输入搜索内容	Q,		请输入搜索内容		
			> 禁用			
	10000000000000000000000000000000000000	8	< 启用	暂无数据		



3.1.6.31 监控端口范围

监控端口范围		
* TCP 鐺口列表 ③	1-85535	+ 导入端口组
UDP 雄口列表 ⑦	请输入正确的 TCP 礁口	+导入端口组
論过不存活主机 ③	请输入正确的 UDP 端口	

- TCP 端口列表:
 - TCP 端口为 1 至 65535。
 - 具体配置方法:
 - ◆ 直接输入端口;
 - 输入端口号,多个端口号之间以英文逗号","分隔;
 - 支持输入端口段,如:"10-18"。
 - ◆ 导入端口组:
 - 点击"+导入端口组";
 - 在弹窗中选中要导入的端口组,点击"确定";
- 端口组中的端口会自动加入当前的端口列表后方。UDP 端口列表:
 - UDP 端口为 1 至 65535。
 - 具体配置方法:
 - ◆ 同上 TCP
- 跳过不存活的主机:
 - 启用后,对于主机存活探测中发现不存活的主机,任务不会再尝试扫描;
 - 否则任务会不考虑主机存活状态,直接尝试扫描所有主机。
 - 关闭时可能导致扫描速度大幅下降。


3.1.6.32 监控白名单配置

开启后,排除扫描目标中不进行漏洞检测或者不进行资产发现的目标。

监控白名单配置		(BR)
* 不监控的主机	白毛单格式, 回车换行分离 1.1.1.1 1.1.1.1/24 1.1.1.255 domain.com 200100b8:3o4d:0015:0000:0000:1a2f1a2b http://www.chailin.cov https://www.chailin.cov	导入主机资产

- 检测白名单:
 - 按照格式要求,手动填写不想进行漏洞检测或不想进行资产发现的目标地址;
 - 或通过点击"导入主机资产"导入目标地址。



3.1.6.33 检测内容设置

监控内容设置

开启漏洞扫描

● 开启漏洞扫描



3.1.6.34 漏洞探测插件

可以在此自定义任务启用的插件。

		- I	混消插件								×		admin
MAINE	~	CENTRAL (C)											
- XONAR		新市休 市	minis or .	而在成別開社中的大学的	ait, mila	产并增加打扫描有限	1277日新教教室文件整要等风险, 1	LETHIRTY.					
-		- And the state	课则条应			湯河嶋号		漏涡炎型		講問标題			
10040		-	還到該選打員	用他们	80		10.000 CI	福作古印		通件标题			
Constant.		Western Street S	譜件风险			福件更新时间	2116 CE 301	1	MREM C				
		1	 已透祥 	9006 个课用操作									
				建用量件名称	#12	操作风险	徽件标签		赢用标签		續件更新时间		
DIRA				CVE-2018-2022-Dec		20.00 to	SERA BART HER	100	BRING DEPENDING (CM)		2024.02.18 16:31:36		
"大学时和48			1120			ingeneral.							
2 2***			•	CVE-2023-24488: Cl	内量	无风险	大市市		OTIVIES CONSIDER AND		2024-02-18 15:57:36		
* 2012-02			8	CVE-2022-4057: Wo	PAT	75.NUR	ARR		MH11H		2024-01-10 18:17:05		
3 5810			8	CVE-2022-4040: Wb	内育	无利地	2.0.8		18492108		2024-01-10 18:17:07		
C ana				CVE-2022-48022: Z	内面	3.802	A.8.8		meren		2024-01-10 18:17:07		
O KARIE				神道项目管理系统/4	11.00	无风险	无效調		are steam speeze a		2024-02-05 16:32:19		
A WORK				CVE-2022-45205: Je	内面	光用脸	大地湖		20"R 81202 7342 AS		2024-02-05 18:32:19		
				海豚底花 NNAS-8700	11.00	0,000	文件上作 (由浦相)		MAR BRON RHEE AR		2024-02-06 18:26:21		
				CVE-2020-24958: ML	内景	无风险	2.5.8		manne waaaten (cent		2024-01-10 18:17:05		
				OVE-2023-30061: D	内田	无风险	5.11.8		J# 49 (216)		2024-01-10 18:17:05		
								具 3170 集	: 1 2 3 4 5	317 >	10 %/% - 18.52 JI		
					_			_			12 M (8 M	0000E6	

- 不同的插件可以探测不同的漏洞。
- 可以在漏洞等级、漏洞编号、漏洞类型、漏洞标签、漏洞披露时间、插件名称、插件标签、插件风险八个维度进行对插件的筛选
- 根据插件选择情况展示可能扫描到漏洞的总数,对应四种风险等级的数量
- 版本匹配配置
 - 支持对版本匹配的漏洞进行进一步选择
 - 每次扫描最大支持选择 2000 条漏洞
 - 支持筛选

选择要匹配的漏洞	 已选择 0 个漏洞 		清空已;
漏洞名称	漏洞等级	影响资产组件	操作
		暂无数据	



入要匹配的漏洞					
● 由于任务扫描以及	及产品性能的考虑,每次下发任务最多选择 2000 个版2	4匹配漏洞			
洞名称:	漏洞编号:		漏洞等级:	v)#	洞标签:
定义标签:	影响组件:		影响服务:		
	瀾淵名称	漏潤等级		影响资产组件	
	金螺产品 js 任意文件读取漏洞	80		金螺云-精斗云-财务软件	
	碧海威 confirm.php 远程命令执行澜润	6		公司产品	
	Alibaba Nacos 歸口令瀧洞	**		Alibaba Nacos	
	朗驰欣创视频监控系统登录绕过漏洞	而用		的地欣创视频监控系统	
	帮管客CRM /init 信息泄露漏洞	R R		蒂普客-CRM	
	帮警客CRM /jiliyu SQL注入漏洞	R B		帮管客-CRM	
	用友GRP-U8 operOriztion SQL注入灑淵	現几		用友 GRP-U8	
	上海普华科技发展股份有限公司PowerPMS存在	**		蕾华科技-PowerPMS	
	成都任我行软件股份有限公司管家婆分销ERP系	#/L		管家婆订货易	
	契约锁-电子签章系统 /utask/upload远程命令执	6		契约锁-电子篮章系统	
0 已选择 0 个漏洞				< 1 2 3 4 5 ····	26432 > 10条/页~ 跳至]

3.1.6.35 自定义弱口令猜解字典

任务扫描 Web 弱口令漏洞时, 默认使用智能弱口令字典探测。启用"自定义弱口 令猜解字典"后,则可以自定义扫描 Web 页面时的弱口令探测字典。如何配置自定义 字典,可以参考 3.1.4.1 字典管理 中的说明。

注: 自定义弱口令探测字典,只有在"漏洞探测插件配置"中, 启用"Web 表单 弱口令漏洞扫描插件"时才能生效。

自定义弱口令猜解字典		SH
	用户名字典	v.
	密码字典	

- 用户名字典:
 - 选择探测弱口令用户名时使用的字典;
 - 字典内容一般选择常见的用户名:
 - ◆ 如 admin、root 等;也可以尝试选择企业、组织内部的默认用户名,比

如工号、学号、电话号码等。

- 密码字典:
 - 选择探测弱口令密码时使用的字典;
 - 字典内容一般选择常见的弱密码;
 - ◆ 比如 123456 等。

3.1.6.36 自定义路径猜解字典

当目标 Web 页面上的链接不多,或者有很多独立页面时,字典猜解可以作为 Web 爬虫 的一个很好的补充,帮助任务收集网页信息。

当"自定义字典猜解"关闭时,任务默认使用智能的字典猜解模式;启用时,则可以自 定义扫描 Web 站点时的路径猜解字典。如何配置自定义字典,可以参考 <u>3.1.4.1</u>字典管理 中的说明。

注: 自定义字典猜解,只有在"漏洞探测插件配置"中,启用"自定义字典信息泄 露漏洞检测插件"时才能生效。

自定义路径猜解字典				
路径猜解字典				v

- 路径猜解字典:
 - 选择路径猜解时使用的字典;
 - 选择后,任务会尝试用字典中每一行的内容作为目录,猜解扫描目标:
 - ◆ 如,扫描目标为 http://www.test.com,路径猜解字典每行分别为 /a /、

/b/、/c/。则任务会尝试猜解 http://test.com/a/、

http://www.test.com/b/、http://www.test.com/c/ 页面



3.1.6.37 自定义弱口令配置

自定义弱口令配置 ①						
MARE ()						
	* 颅户名字典					
	* 医药学典					
	INTERACE O					
	单个脑性增强进时时间 ①	诸据人大学专用部数,不可能认为	ABB			p
	连续爆破时间署 ①	· 由国人大于10月18日,平均国际内	无限制			Ð
	直续爆破最大次数 〇	warit comm. Samir	A.81%			
	每秒最大爆破次数	IIIIAAFAWIIR, 平田1035	齐阳 帆			
	* 单次口令爆破请求发送起时时间	3				ю
	* 单次口令爆破朝后读取版时时间	3				ø
	全量学典博敏 ③	C10				
服务	用户名字	A	思码字典	全量字員爆破	18 1 5	
			10王20-02			

- 用户名字典
- 密码字典
- 单个插件爆破超时时间
 - 填写大于0的数字,不填写则代表无限制
- 最大连续爆破次数
 - 填写大于0的数字,不填写则代表无限制
- 连续爆破时间窗
 - 填写大于0的数字,不填写则代表无限制
- 每秒最大爆破次数
 - 填写大于0的数字,不填写则代表无限制
- 单次口令爆破请求发送超时时间
- 单次口令爆破响应读取超时时间
- 全量字典爆破:对字典全匹配进行爆破尝试,会增加扫描时长
- 特殊配置:
 - 为某个扫描对象单独配置参数
 - 具体操作:
 - ◆ 点击"+添加特殊配置",跳出弹窗;
 - ◆ 在"配置服务"中选择目标对象;
 - ◆ 其余参数同上;
 - ◆ 点击"保存", 完成配置。
 - 保存的配置会一直存在,可选操作:



- ◆ 编辑
- ▶ 删除

* 配置服务	SSH 弱口令漏洞检测插件	
* 用户名字典	SSH 用户名字典	
* 密码字典	SSH 密码字典	
单个插件爆破超时时间 ②	请输入大于 0 的整数,不填默认为无限制	
连续爆破最大次数 ⑦	请输入大于 0 的整数,不填默认为无限制	
连续爆破时间窗 ⑦	请输入大于 0 的整数,不填默认为无限制	
每秒最大爆破次数	请输入大于 0 的整数,不填默认为无限制	
* 单次口令爆破请求发送超时时间	3	
* 单次口令爆破响应读取超时时间	3	
全量字典爆破 ⑦		

3.1.6.38 自定义域名猜解字典

进行域名发现时,域名猜解是是发现子域名的重要方式。

当"自定义域名猜解字典"关闭时,任务默认使用智能的域名猜解。启用时,则可以自定义子域名的猜解过程。如何配置自定义字典,可以参考 <u>3.1.4.1 字典管理</u>中的说明。

自定义域名猜解字典)
域名猜解字典	
是否允许递归猜解	
递归猜解字典	

- 域名猜解字典:
 - 选择域名猜解时使用的字典;
 - 选择后,任务会尝试使用字典中每一行的内容作为子域名,去猜解目标域名。
 - ◆ 如, 域名目标为 news.example.com, 字典每行分别为 test1、 test2、

test3。则任务会尝试猜解 test1.news.example.com、

test2.news.example.com、test3.news.example.com 等域名。

- 是否允许递归猜解:
 - 开启时,任务在第一层域名猜解成功后,会对猜解到的域名,继续进行递归猜 解。
- 递归猜解字典:
 - 选择开启递归猜解时使用的字典。



3.1.6.39 其他检测选项

其他检测选项	
通过云服务收集信息 🗇 🦲	
探测域名传送漏洞 🔵	
自动发现 Web 站点 ⑦ 👥	
基于关联关系的子域名收集 ③	

- 通过云服务收集信息:
 - 启用时,任务会尝试使用公开、免费而可靠的第三方云服务收集目标的信息;
 - 通过云服务收集是子域名发现重要的补充手段,可以突破域名猜解固定字典的限制,收集到不在字典内的子域名信息。
- 探测域名传送漏洞:
 - 启用时,任务会尝试探测 DNS 服务器是否存在域名传送漏洞,以借此收集域 名信息;
 - 域名传送漏洞是指由于 DNS 的配置不当,导致某个域的所有查询记录泄露 给匿名用户。域名传送漏洞如果存在,则是一个有效的收集域名的方法。
- 自动发现 Web 站点:
 - 启用后,任务会自动探测发现的每个域名下是否有对应的网站;
 - 很多域名都直接对应一个网站,如果需要收集一整个域下的网络拓扑结构,使 用域名资产发现策略,并开启自动发现 Web 站点,是一个简单而全面的方法;
 - 当然,如果并不需要 Web 站点信息,可以关闭"自动发现 Web 站点",这 样能减少任务耗费的时间。



3.1.6.40 URL 去重设置

URL 去重设置		
* 去重时间窗	2	-j-83
自定义去重方式	2 対 URL 中的大小写戰滅	
	保羅 URL 中的 HASH 部分	
	□ 保留 URL 中的 QUERY 部分	
	2 智能识别 URL 撇写	
去重设置适用阶段	2 测润检测的投	
	2 资产发现阶段	

- 去重时间窗:
 - 用于设置去重的时间间隔
- 自定义去重方式:
 - 对 URL 中的大小写敏感:默认开启
 - 保留 URL 中的 HASH 部分:默认关闭
 - 保留 URL 中的 QUERY 部分: 默认关闭
 - 智能识别 URL 重写: 默认开启
- 去重设置使用阶段:
 - 漏洞检测阶段:
 - ◆ 在漏洞检测阶段使用此处的去重配置信息。
 - 资产发现阶段:
 - ◆ 在资产发现阶段使用此处的去重配置信息。
 - 注:基本 Web 漏洞扫描, 被动 Web 扫描(镜像) 无该选项组



3.1.6.41 全局白名单选择

<・>洞鉴 _{x-RAY}					admin
默认工作区 V 日本世界	1 / 任务列表 / 添加扫描任务				
② 全局仪表盘		推定时间段 ② 💿 指定扫描	时段 📋 指定禁扫时段		
日相接管理		超始时间		 	
任然统计		激励相定时间和			
EIRINA					
任务改奏	全局白名单选择				
扫描设置 ~					
字典管理	🔽 - 全局白名单启用	白名单名称	白名单媒述	创建组织单位	操作
编口经管理		test456		默认工作区	
全局白名单配置	2	test123	+	脱认工作区	
当打平台监听配置					< 1 > 10条/页∨
A 基线管理 ~					

- 根据当前工作区可获取到全部的全局白名单(应用配置开启并且该工作区在应用配置范围内)
- 不勾选全局白名单,即禁用,任务循环执行时不再应用该全局白名单。
- 可查看白名单:

查看扫描白名单	
トクかかか	h
日名早名称	test456
白名单描述	
所属组织单位	默认工作区
规避扫描的主机目标	
规避扫描的 Web 目标	
扫描白名单适用	不进行资产发现、不进行漏洞检测
URI 禁扫关键字	delete,remove,logout
应用配置	开启,同步应用到子组织单位



3.1.6.42 扫描时间配置

扫描时间配置							
	*执行类型 💿 立即扫描	🔘 定时扫描一次	🔿 每天循环扫描	- 每周循环扫描	○ 毎月循环扫描		
	指定时段 ③						

执行类型:规定此任务时间窗从什么时候开始。
 ■ 立即扫描

*执行:	类型 💿 立即扫描 🔵 定时扫描一次 🦳 每天循环扫描 🔵 每周循环扫描 🤄 每月循环扫描
指定时段	20
■ 定时扫描—次	7
	\mathbf{N}
- 人EHJ]-J]田 八 配置	立即扫描 • 定时扫描一次 每天循环扫描 每周循环扫描 每月循环扫描
- 人ビドリコーゴ田 ·ハ 配置 * 执行类型 * 开始扫描时间 ③	 立即扫描
- 人EHJJ-JJ田 《人 配置 * 执行类型 * 开始扫描时间 ③	 立即扫描 定时扫描 、 毎月循环扫描 2023-04-26 11:24 2023-04-26 11:24 日満在秀创建成功后,将在 2023-04-26 11:24:00 开始执行

■ 每天循环扫描

* 扶行黄鬘 立即扫描 定时扫描一次 • 每天循环扫描 每周循环扫描 每月循环扫描	
* 开始扫描时间 11:25 扫描任务从现在开始,每天的 11:25:00 循环执行扫描任务	
milen o	

■ 每周循环扫描



*执行类型	◎ 立即扫描 ◎ 定时扫描一次 ◎ 每天循环扫描 ● 每周循环扫描 ◎ 每月循环扫描	
* 开始扫描时间	周 11:25	
	扫描任务从现在开始,每周周一的 11:25:00 循环执行扫描任务 适加时间	
#定时限 ◎		
#定时段 ◎ ■ 每月循环扫描		
^{指定时段} ◎ ■ 每月循环扫描 描时间配置 * 执行类型	 立即扫描 定时扫描 定时扫描 一次 每天循环扫描 每周循环扫描 ● 每月循环扫描 	
^{指定时段} ◎ ■ 每月循环扫描 描时间配置 * 执行类型 * 开始扫描时间	 立即扫描 定时扫描 一次 每天蘸环扫描 每周循环扫描 ● 每月循环扫描 ● 每月循环扫描 ● 有月 年 11:25 	

- 指定时段:开启后,可以选择指定扫描时段或者禁扫时段实现对任务扫描时段的控制可以选择指定扫描时段或者禁扫时段实现对任务扫描时段的控制。和执行类型的 开始扫描时间不冲突。
 - 可添加"每天"/"每周"/"每月"的扫描时间段或设置为"禁扫时段"。

*	执行类型	 立即扫描 	〇 定時	寸扫描—>	次 〇	每天循环扫描	0	每周循环扫描	○ 每月循环扫描	â
指知	定时段 ⑦									
		每天~	起始时间		~	结束时间				
			起始时间		~	结束时间		0		
•	每	 通知时间段 通: 应用为禁护 至天: 	空所有时段							
* 执行类型 指定时段 ⑦	 立即封 	3描 🔘 定时	扫描一次	0 4	天循环打	3描 () 每)	周循环打	3播 🔘 毎月	目循环扫描	
	每天▽	超始时间		~	结束时间	i 0				
		起始时间		~	信期时间	0	0			
	添加时间段	潭空所有时段								
	应用为	辨扫时段								
•	每	. 周:								



 毎周〜 起始时间 ○ ~ 結束时间 ○ 日 一 二 三 四 五 六 あか时间段 通知方候扫时段 	指定时段 ⑦ 🛑
總加約司段 应用为禁扫时段	毎月→ 起始时间 ○ ~ 桃東时间 ○ 日 一 二 三 四 五 六
应用为禁扫时段	加加时间段 演变所有时段
	应用为禁扫时段

◎ 执行类型	1 💿 立即扫描	2 定时扫描一次	○ 每天错	环扫描 📿	每周循环扫描	() 每月	循环扫描		
指定时段(
	毎月▽	按第几个周几小	假始时间	0 -	* 结束时间		选择应用日		
	Witering a	按每月第几日							
	THE R	按第几个周几							

可按照"第几个周几"和"每月第几日"选择指定时段。如果月份中不存在选中的天, 那么在该月则不会进行扫描任务。

备注1:参数使用第5个周几的发布任务存在扫描风险,因为每个月不会存在涵盖 所有的第5个周一到周日,所以尽量规避设置在第5个周几。

备注 2: 参数使用第几个周日的发布任务存在扫描风险,尽量规避设置在第几个周日。



3.1.6.43 其他插件配置

其他插件配置	
启用盲打平台 ⑦	查看引擎盲打平台配置详情
* web漏洞检测深度 ⑦	2
*最大并发插件数	30
智能插件调用 ⑦	
智能播件调用 ③	

- 启用盲打平台:
 - 主要用于插件对无回显漏洞对验证;
 - 辅助扫描插件输出结果中对无回显漏洞。
 - 正常通信前提需要对盲打平台进行配置,点击"前往配置盲打平台"可前往进行配置,详情配置信息可见 <u>3.1.4.3 盲打平台监听配置</u>。
- 设置 Web 漏洞检测深度
 - "?"提示:设置漏洞插件对 web 目标资产拼接前的路径的深度的限制,默认为
 - 2, 设置范围为1-10。
- 最大并发插件数
 - 支持对所选漏洞插件最大并发数量做限制
 - 默认 30
 - 设置范围为 1-100
- 智能插件调用
 - "?"提示:根据资产指纹识别的结果,进行精准的漏洞探测,扫描速度会有所提升;基础服务扫描需要手动开启指纹识别,以提高资产指纹识别准度,web 扫描默认开启指纹识别

3.1.7 代理服务器配置方法

配置好代理服务器后,就可以使用被动 Web 扫描了。

具体步骤为:

- 添加一个被动 Web 扫描任务,填写需要扫描的目标站点。根据所需配置其他参数,并保存任务;
- 启动任务,此时任务详情页面将展示 HTTP 代理服务器的 IP 地址和分配的端口号;

长李科技总部	Y	HIRTON / G-MPUM / WK							
13181878		测试		結果对比	和辅历史 •	STELLER 2	的服務性	暂停信息收集	伊止日期
任务统计									
扫描開始		低条统计 漏洞 (0) 城名 (0) 王佑 (0) 服务 (0) Web 站点 (0)							
任务列表									
白细胞胃		IINIAR			任务基本信息				
自定文 POC 列	a.	唐彦建公平 HTTP 伊爾诺丹信息武庫:149-26411:80			任务状态	正在扫描			
資产中心		使用HTTP代理后可提合影响客户课使用HTTPS的网站,下量HTTPS都证布并安装可解决该问题。		001	扫描用的	被动 Web 扫描(代理))		
湖川碧田		最近 20 秒平均和20 HIGh: Dees		0.26	此动时间	2021-01-07 18:05:55			
经告销理					EDIDATION	1			
系统设置	.*.				20.71E4	398			
系统信息	*	138116	下载日春	含氧更多	已归援 URL 對量	٥			
基线管理		(14(45:55) (秋志堂書)) 任美 [102] - 英雄四期 -> 英雄田田, 東田 平山田市			已放出 HTTP 面水面	0			
用户管理		(18(65:55)(以此意思)(任务[18(2])(各項[18] → 正有[18], 第(3))并及[28(4]] (18(65:55)([18(279)])			已采集 LiniL 数量	G			
日之軍項		 [10:05:05] (1498(第) (第) 28) - 0+094-08806974753414-04-0182144-754 [10:05:05] (2898(第)) [10:05:05] (2898(第)) [10:05:05] (288(第)) [10:05:05] (288(第)) [10:05:05] (288(第)) [10:05:05] (288(第)) [10:05:05] (288(第)) [10:05:05] (288(28)) 			重正打运商				

- 这时用户需要打开自身客户端系统网络设置,或者浏览器的网络配置,将网页的代理服务器设为任务详情页面显示的代理服务器。
 - Mac OS 系统可在系统偏好设置 / 网络 / 高级 / 代理中设置:



请选择一个协议进行配置:		安全网页代理服务	22				
□ 自动发现代理		25.25.206.26	: 32780				
 自动代理配置 回 回声代理 (UTTD) 		代理服务器要求密码					
 ☑ 安全网页代理 (HTTPS) 		用户名:					
□ FTP 代理		密码:					
□ SOCKS 代理 □ 流代理 (RTSP)		您的须	证可能以不加图方式发行	ž			
□ Gopher 代理							
不包括简单主机名 忽略这些主机与域的代理设计	E :						

 Windows 可以在控制面板 / 网络和 Internet / Internet 选项 / 链接 / 局域 网 设置中,选择"为 LAN 使用代理服务器":

目动配置 自动配置会覆盖手动设置	。要确保使用	手动设	置, 请结	朝自动配置。
✓ 自动检测设置(A)				
□使用自动酸(置脚本 (S) 地址 (B)				1
代理服务器				4
☑ 为 LAN 使用代理服务	器(这些设置不	「用于找	(号或 VI	'N 连接)(X)
地址(四): 10.3.0.16	端口 (T):	80	I	高级(C)
]]跳过本地地址的代理	服务器(B)			

 用户也可以直接使用支持自定义代理的浏览器,如 Chrome 浏览器的插件 SwitchyOmega。



▶ 界面	代理服务器	Ŧ						
✿ 通用	网址协议	代理协议 代理服务器		代理端口				
₩ 导入/导出	(服天主人)	HTTPS	\$ 25.25.206.26	32780	٢			
5景模式	▼ 显示高级	✔ 显示高级设置						
😪 proxy								
	小代理的耶	亚列表						
th auto switch	7/7/4/000/#		△ + 40.					
LT auto switch + 新建情景模式	不经过代理连 (可使用通配符	接的主机列表: (每行- 等匹配规则)	-个主机)					

- 配置好客户端的代理服务器后,就可以用客户端的浏览器打开需要扫描的目标站点,依次访问自己希望扫描的页面,
- 回到之前的扫描任务处,可以看到任务通过代理收集的信息,并且同时进行漏洞探测;

注意:

● 使用 HTTP 代理可能会影响客户端使用 HTTPS 的网站, 在扫描详情页或全局配

置页可以下载 HTTPS 的根证书, 安装并信任后可以解决该问题 (如下两图所示):

长亭科技总部	¥	DISTR CENTR MIX							
扫描管理	*	测试	ABRIVIT	招赐历史 ¥	· 编辑扫描任务 哲学家异位言	1948.63	9 止日後		
任务统计		A							
的建筑		任务48.17 派派 (0) NEG (0) 主机 (0) NES (0) Veeb 31.6 (0)							
任务列表									
白塔配置		EN MARK		任务基本信息					
自定文 POC 列曲		REALITY ATTA PRODUCT PROPERTY AND A LODGE		任务状态	正在扫描				
肥 产中心		使用 HTTP 化理测可能会影响客户理使用 HTTPS 的间站,下在 HTTPS 机位用 安装可解决该问题。		111230.00	補助 Web 扫描(代理)				
演判管理			0%	直动时间	2021-01-07 18:07:40				
按应管理				1338P215	00:00:28				
系统设置	•			運用通信	396				
系统信息		日曜日本 下載日本	R#世5	EIERE URL BUB	a				
基弦管理		the state of the last a same a same and the		已放出 HTTP 像水路	0				
用户管理		[10:07:04] [10:02(1)] 任命 [10:03] · 如何100 · 日前100 · 日前		已早期 URL 教皇	0				
8584		<pre>(International Control of Co</pre>	ver, errs i referen	S. ETING					



长率科技总部	×	INTER COMPLETE MARANARE	
扫描管理 (F&欲))		被动爬虫服务器配置	
1310100		SITTA	引導作点 168-254.1.1
(181)8		100.254.1.1	基于代理的描述理由的代理服务相能置
日本記載			以下代理最非裁,用于为被益 Web 或用目指任务提供需要的代理服务都信息,如以指口目的可以提先的大增等间信配置对组务间口的情绪,不堪表示无限制。希任务单 输配置了指口因用,的优先使用任务配置,
重打平台店	SER.		代增展角档 # 169.254.1.1 🖉
被动用出来			BY LANCIEN · Z
HENTE	200		使用 HTTP 代現后可能做影響和Paik使用 HTTPS 的网络。下槽 HTTPS 相亚将并安装可能决该问题。
字典管理			HTTPS 根亚市 直击下他 HTTPS 相证书
180日安存			基于日志的被动骤虫的 Synolog 易奏器配置
-			以下 flytting 服务器,而于为属于日志的接动 Web 属和白油任务提供需要的代理服务器组集。
ee.rsre			Systing 服务器 IP 199 254.1.1 2
BIEX POG N	(A		
豊产中心			
展刊管理			
报告管理			It Ray 101-0110 manter 02 2000 Charley from
系統设置			
系统信息			
基线管理			
用户管理	*		

 代理服务器的端口在被动 Web 漏洞扫描的任务开始时会自动分配。任务结束后, 端口将被自动收回。请注意每次开始一个被动 Web 漏洞扫描的任务时,都需要重 新配置客户端的代理设置。



3.1.8 API 扫描文件获取方式

3.1.8.1 接收地址 配置说明

访问在线 swagger 文档的链接,可在图中标红的输入框中获取

(e) Swagger	https://petstore.awagger.io/v2/swagger.json	Explore
Swagger Pet	store 💷 🚥) via 1 zivin	
This is a sample server Potstore titions. Terms of service Contact the developer Apache 2.0 Find out more about Swegger	ever. You can find out more about Biesgger at <u>http://teesgger.ip</u> or on <u>incl.fisecode.ort</u> , <u>Biesgger</u> . For this se	emple, you can use the api key special-key to test the authorization
Scherres HTTPS >		Authoriza 🔒
pet Everything about your P	5	Find out more
<pre>dif /pet/{petId}</pre>	Find per by ID	ii ∨
POST /pet/{petId}	Updates a pet in the store with form data	ê ∨
DELETE /pet/(petId)	Deletes a pet	≜ ~
POST /pet/{petId}	uploadImage uploads an image	ê ∨
POST /pet Add a new	et to the store	≜ ~
Inter Court Lindstein	dition pet	1 V

注: 仅限于用 swagger 工具进行开发管理接口的情况,其他情况使用"文件上传"的方式

3.1.8.2 文件上传 配置说明

方式一:

通常可以在 swagger UI 界面左上角找到以".json"结尾的 URL

链接处右键,保存为".json"格式文件



Swagger	https://petstore.swagger.io/v2/swagger.joon	Explore
Swagger Petsi I have the petsion wagers and important and any of the same target / petsion wave field on server targets	(You can find out more about Swagger at http://twagger.is or on instructede.oet. Bissagger, For the	s sample, you can use the spillery $\ \mbox{specIal-key}$ to test the authorization
Scherres HTTPS ~		Authoritas 🔒
pet Everything about your Pets		Find out more
Gitt /pet/{petId} Find	per by ID	ê ∽
POST /pet/{petId} Upd	ates a pet in the store with form data.	ê ∽
DELETE /pet/{petId} Des	teo a per	≜ ∨
POST /pet/{petId}/up1	oadImage uploads on image	â V

方式二:

当界面没有 URL 链接时, 可通过 F12 打开浏览器控制台, 然后定位到 [Network -> Fetch/XHR] 后刷新页面, 找到 ".json" 格式的文件

双击访问页面,在空白处右键,保存为".json"格式文件

	(ii) Swagger	https://petstore.swagger.jo/v2	2/swagger.json			Explore	
	Swagger Pets 1 Base URL: petstere, swager, forv https://petstere.swagger.p/et/	tore 🚥 🚥					
	This is a sample server Petstore service.	er. You can find out more about Swagger at ht	to://twogger.ig or on inchreenode.n	et. Exwagger, For this sample	, you can use the api key special	-key to test the authorization	
	Terms of service						
	Contact the developer						
	Apacha 2.0						
	Find out more about Swegger						
	HTTPS *					Authorize 🔒	
F Th Elements Consol	Sources Network Performence Me	mary Application Security Lighthouse	Recentor Performance insights X				01 R L X
🗐 🥥 👎 🤤 🗌 Presens	ve log 🔲 Olsable cache No throtting 🔹 😒						0
Bin D	Invert 🗇 Hide data URLs 🗐 Hide extension	URLS AN FRIENWER Date CBS JB Ford In	rig Media Marifest WS West Ot	🖶 🗄 Blocked response cookie	is 🗇 Blocked requests 🗇 3rd-party n	equests	
200 me 400 ms		ma 1200 ma 1400 ma 1600 m	na 1000 ma 2000 ma	2200 mi 2400 mi			
Nate	× Headers Preview	Response Initiator Timing Costiles					
	 Congager "July, Lines, Marchand Stark, * writernalisers (Baser harts" galantee, long * jorks Gu3 * parties Gu3 * societized actions * man, "Sub- * man," Sub- * ma	(), next: "persen, nagger, or, andfordt" ation: "flad out more about bagger", ort: "At arr.lo" stafi ataril description: "howything about your Pets",).	/we*) ta://www.gar.lo*) : "Nandar")) 1				
1/10 requests 16.1 kB / 16.6 kd	Ritransferred 13.4						
1 Console Whet's new x							
Highlights from the Chrome 125	update						

方式三:



若客户未使用 Swagger 工具进行开发和管理,需要导出以 swagger 格式为准的 json 文件,方可使用

3.1.8.3 注意事项

需要确保 json 文件中包含"host"和"schemas"字段,在某些不规范的开发过程下,导出的文件可能并不包含,需要手动补充添加,才可以实际扫描到接口





3.2 基线管理

Xray 目前版本支持 Linux 和 Windows 的基线检测

3.2.1 基线检查任务列表

在左侧导航栏中,选择"基线管理-基线检查任务列表",进入基线检查任务列表界面。

<->洞鉴 _{x-n}	RAY					admin
默认工作区	✓ 采用型理// 基线检查任务现表					
① 全规仪表盘	在城橋會利義 崇成批量利点 實成本地列表					
日 白銅管理	▼ 「用用用用中位 繁以工作区 ×) + 激烈精透条件					
当 基线管理	▲ ● B透祥 ◎ 个任务 ■新运中的任务 铁行运中的任务 专业运中的任务					+ 流动检查任务
基础检查任务利用	□ - 检查任务名称	检查策略	扫描计划	检查结果	任务状态	操作
基线检查把置			colori			
素酒产中心	v dd	CIS Ubuntu 16.04 Level 1	无	65/159/159	 已完成 	12.21 (0.11) (0.12)
◎ 運用管理	- ⁻ 得到的	CIS CentOS 7 Level 2	无	21/33/33	③ 巴完成	10.00 00.00 94.54
□ 服務中心	× 17.99.235.124	CIS Ubuntu 16.04 Level 2	无	0/0/33	◎ 已完成	1281 (833) (636)
C ROOM	* C 161638	CIS Ubuntu 16.04 Level 1	无	0/0/155	⊙ 已完成	12.01 (0.03 50.02
◎ 系统管理	8				(Ca)	1 10.8/7
A 用户管理	8					The age of the

3.2.1.1 内容展示

基线检查任务列表包括在线检查列表,离线批量列表和离线本地列表,展示系统创建的所有基线检查任务。

在线检查列表

列表包含检查任务名称、检查策略、扫描计划、检查结果、任务状态、操作。

- 任务名称;
- 检查策略:展示实际检查中勾选的检查策略,鼠标悬浮展示全部;
- 扫描计划:展示周期执行时间。鼠标悬浮展示任务执行周期和任务指定执行时间段;
- 检查结果:展示不合格检查项数量/已进行检查项数量/总检查项数量;
- 任务状态:展示任务执行状态;
- 操作:进行检测,编辑,删除操作。



新闻应	40年位 默认工作区 × + 添加筛选条件					
B	选择 0 个任务 副目近中的任务 具行造中的任务 帮上造中的任务					+ 1510档道
	检查任务名称	检查策略	扫描计划	检查结果	任务状态	操作
	dd	CIS Ubuntu 18.04 Level 1	无	65/159/159	③ 已完成	1235 8558 4938
	得到的	CIS CentOS 7 Level 2	无	21/33/33	② 已完成	检测 删除 编辑
	47.98.235.124	CIS Ubuntu 16.04 Level 2	无	0/0/33	② 已完成	检测 删算 编辑
	验验验	CIS Ubuntu 16.04 Level 1	无	0/0/155	◎ 已完成	ACUN INTO SAVE

点击任务所在行,可跳转至任务详情页。

离线批量列表

列表包含检查任务名称、检查策略、检查结果、最后检查时间、操作。

- 检查任务名称;
- 检查策略:展示实际检查中勾选的检查策略。鼠标悬浮展示全部;
- 检查结果:展示不合格检查项数量/已进行检查项数量/总检查项数量;
- 最后检查时间;
- 操作:进行编辑和删除操作。

在线检查列表 廣越批量列表 离线本地列表			
用風班彩車位 默认工作区 ×) + 添加制造条件			
已选择 0 个任务 新闻:这中的任务			+ 液却检查任务
□ ~ 检查任务名称	检查策略	检查结果 最后检查时	司 操作
	留无数图		
			(10 条/页~

点击任务所在行,可跳转至任务详情页。

离线本地列表

同离线批量列表。



3.2.1.2 筛选操作

在列表页可对任务进行筛选操作,可根据扫描任务名称、检查策略、创建时间、任务状态(仅在线检查列表)、最近一次运行时间(仅在线检查列表),自由添加一个或 多个条件进行筛选,操作说明如下:

- 点击"添加筛选条件"按钮;
- 在弹出的添加筛选条件对话框中配置筛选条件:
 - 选择要增加的筛选条件类型并填写相应的要筛选的内容;
 - 点击"添加筛选条件",可以增加新的筛选限制条件;
 - 点击 "删除", 可以删除掉不需要的筛选限制条件;
 - 筛选条件限制至少要添加一条;
- 设置好条件后,点击"保存",筛选条件完成;
- 若想删除筛选条件,点击已添加条件右侧的"删除"按钮,即可删除条件。

在线检查列表 高线批量列表 高线本地列表					
Auguston MULTRE × + 2017					
● 已选择 0.个任务 新程造中的任务 执行遗中的任务 停止遗中的任务					+ 惑加检查任务
□ ✓ 检查任务名称	检查策略	扫描计划	检查结果	任务状态	操作
bb D	CIS Ubuntu 18.04 Level 1	无	65/159/159	③ 已完成	10.00 0000 00.00
() 领到的	CIS CentOS 7 Level 2	无	21/33/33	◎ 已完成	10.00 9009 5818
47.98.235.124	CIS Ubuntu 16.04 Level 2	光	0/0/33	③ 已完成	10.20 80.08 54.18
□ 除約6	CIS Ubuntu 16.04 Level 1	无	0/0/155	② 已完成	检测 删除 编辑

检查任务名称	Y	请输入要筛选的内容	
+ 添加筛选条件			



3.2.1.3 删除操作

在列表页可以对任务进行删除操作,一旦执行删除操作,所有已选任务的删除条目 均无法恢复,有以下两种途径:

■ 单个任务删除,

■ 批量删除操作

在线检	童邦表 高线赴量列表 离线本地判表						
instat	村未去而此款 + X 就就还面刻递要不能 1000						
• E8	1種 B 个任务				批量操作 >	+	活加检查任
	检查任务名称	检查策略	扫描计划	检查结果	樹除 1 応司	18175	
	10.3.0.8	CIS Ubuntu 16.04 Level 1	ž	67/155/155	停止	12.18 81	18 1611
	CIS-Ubuntu-16.0-Lawel-1	CIS Ubuntu 16.04 Level 1	Æ	67/155/155	◎ 已完成	10.00 MI	
	10.3.0.8	CIS Red Hat 6 Level 1,CIS	无	402/896/896	② 已完成	1238 BI	13 1411
	10.3.0.8	CIS Ubuntu 14.04 Level 1,Cl	^夫	349/740/740	② 已完成	10.78 BIT	18 5638
	10.3.0.4	CIS CentOS 7 Level 1, CIS C	无	48/122/1835	② 已完成	12.01 817	88.92
	【不要扫描】	CIS CentOS 7 Level 1,CIS C	无	6/14/1889	◎ 已完成	-	19 1912

3.2.1.4 立即扫描(仅在线检查列表)

对非队列中、进行中的任务,可以执行检查的操作,有以下两种途径:

- 单个任务执行检测,具体步骤为:
 - 点击任务右侧操作栏的"检测",即可进行立即扫描的操作。任务扫描状态变为 等待扫描或者正在扫描。
- 在列表页可以对任务进行批量检测操作,具体步骤为:
 - 选中要执行的扫描任务,此时会显示已选择的扫描任务总数;
 - 点击"执行选中的任务",则任务扫描状态变为等待扫描或者正在扫描,弹窗显示提示;
 - 若选中任务存在"队列中"、"进行中"状态,则跳过该任务。

這检查判表 高线把量列表 高线本地列表					
風雨雨垂症 请不要删除游试数据 × + 添加得送条件					_
● 已选择 6 个任务				批願操作 〜	+ 1510
2 检查任务名称	检查策略	归接计划	检查结果	新聞 4 店动	操作
10.3.0.8	CIS Ubuntu 16.04 Level 1	Æ	67/155/155	停止	1038 BIR 14
CIS-Ubuntu-18.0-Lavel-1	CIS Ubuntu 16.04 Level 1	无	87/155/155	② 已完成	12.5 BIB M
10.3.0.8	CIS Red Hat 6 Level 1,CIS	无	402/896/896	0 CRA	12.0 MIN 14
10.3.0.8	CIS Ubuntu 14.04 Level 1,Cl	充	346/740/740	② 已完成	-
10.3.0.4	CIS CentOS 7 Level 1,CIS C	£	48/122/1835	⊙ 已完成	-
[不要扫描]	CIS CentOS 7 Level 1,CIS C	ž	6/14/1889	② 白完成	-



注意:

- 进行立即扫描的操作后,任务将按照最新保存的参数配置进行扫描;
- 系统正在扫描的任务达到了最大并发任务数时,新启动的任务将进入等待扫描状态。

3.2.1.5 停止扫描(仅在线检查列表)

对正在扫描或等待扫描的任务, 在列表页可以进行单个或批量停止扫描的操作, 具体步骤为:

- 选中要停止的扫描任务,此时会显示已选择的扫描任务总数;
- 点击"停止选中的任务",则弹窗显示提示"所有选中任务已停止",停止的任务
 状态显示为已完成。

3.2.2 检查任务详情

在任务详情页可以查看任务执行进度、任务配置和检查结果,以及离线批量和离线 本地检查模式下的相关操作,还可对任务进行启动、停止、编辑等操作。

6 23	88年位 默认工作区 × + 添加等选条件 选择 0 个任务 新能选中的任务 执行选中的任务 停止选中的任务					+ XXtokia
	检查任务名称	检查策略	扫描计划	检查结果	任务状态	操作
2	dd	CIS Ubuntu 18.04 Level 1	无	65/159/159	◎ 已完成	PERMI MILITY MILITY
3	(積至)(約)	CIS CentOS 7 Level 2	无	21/33/33	⊙ 已完成	HARN MILLS SALVE
	47.98.235.124	CIS Ubuntu 16.04 Level 2	无	0/0/33	⊙ 已完成	10,00 80.08 48.18
	能能验	CIS Ubuntu 16.04 Level 1	光	0/0/155	② 已完成	1231 803 5436

3.2.2.1 内容展示

页面分为任务时间轴、任务风险评级、任务进度、任务基本配置、任务结果、检查 结果概览、风险项情况、风险主机情况、离线检查操作(仅离线检查任务)等模块。

说明:对于离线检查,初始下发任务后,任务统计处无数据显示,需要管理员按照 离线检查操作中的内容进行手动操作任务下发后,将 output.json 上传后,才会显示相 应数据。



	任务风险评	Ω.			任务进度				
(高危 基核粮查任 可以利用这	务已发现多个不安全配置项,累 些漏洞,给您造成业务损失	计评分小于等于 85 分。	高意用户可能 	已检查内容: 159 / 159		100		
基本配置					任务结果				
创建人	admin	创建时间	2021-12-03		检查成功率	风险检查项	不合格主机数		
执行方式	不定时扫描	结束时间	2021-12-03		1/1	65 / 159	1/1		
	风险项情况 风险 相查预能行利 Q 😈 仅3	主机情况 显示风险结果							
		检查结果	检查项总数	风险项		风险爆务器	操作		
宣策略									

任务时间轴,展示扫描历史。

- 在非展开状态下,时间轴包含标题、时间说明、展开操作;
- 点击展开,在展开状态下,以柱状图形式展示最近扫描记录,横轴为时间,纵轴为 个数。
- 单次检查记录数据包括:
 - 风险主机数
 - 安全主机数
 - 未知主机数

任务风险评级:

- 以圆环图显示高、中、低风险的数量排列,数量为检查项的数量;
- 对风险进行评价,评价分为严重、高危、中危、低危、info 五个等级,评级说明、 评价标准和计算方式如下:
- 评价标准:
 - 严重:基线核查任务已发现多个不安全配置项,累计评分小于等于75分,恶 意用户可能可以利用这些漏洞,给您造成业务损失;
 - 高危:基线核查任务已发现多个不安全配置项,累计评分小于等于85分,恶
 意用户可能可以利用这些漏洞,给您造成业务损失;
 - 中危:基线核查任务已发现一些不安全配置项,累计评分小于等于95分,恶
 意用户可能可以利用这些漏洞,给您造成业务损失;



- 低危:基线核查任务已发现少量不安全配置项,累计评分在95~100分区间, 恶意用户可能可以利用这些漏洞,给您造成业务损失;
- 安全:基线核查任务暂未发现存在不安全配置项,您的系统较为安全,请继续保持;
- 未知:基线核查任务暂未发现存在不安全配置项,但存在未知检查结果,请仔 细确认结果。
- 评价标准:
 - 脆弱性元素分值
 - ◆ 每有一个严重,分值-5
 - ◆ 每有一个高危,分值-1
 - ◆ 每有一个中危,分值-0.5
 - ◆ 每有一个低危,分值-0.1
 - ◆ 每有一个 info, 分值- 0.01
 - 资产或任务评分标准
 - ◆ 总分为 100 分
 - ◆ 安全评级:100
 - ◆ 低危评级: 95 < x <100
 - ◆ 中危评级: 85 < x <= 95
 - ◆ 高危评级:75 < x <= 85
 - ◆ 严重评级: 0 < x <=75
- 计算方式:
 - 当任务开始下发时,任务风险显示为未知;
 - 检查结果 = 通过和未知时,不纳入计算;
 - 当所有检查项均完成执行后,若分值仍为100:
 - ◆ 若系统中存在未知,则评价为未知;
 - ◆ 若均为安全,则评价为安全。

任务进度:

- 进度条和进度百分比:当前已进行检查的检查项数量与此次检查任务目标对象总数的比值;
- 已检查内容:数值展示当前已进行检查的检查项数量与/此次检查任务目标对象总数。

任务状态:

- 运行中──任务正在运行;
- 队列中──任务正在排队;
- 已完成──任务执行完成;
- 已失败──任务因各类原因导致中断检测,直接返回了失败(如网络不可达,超时

等), 鼠标悬浮可出现对应失败的 message 信息。

注意:离线检查任务的任务进度显示为100%,任务状态显示为已完成或已失败。

任务基本配置:

- 创建人
- 执行方式:离线显示"-"
- 基线模式
 - 在线远程基线检查
 - 离线批量基线检查
 - 离线本地基线检查
- 创建时间
- 结束时间
- 运行时长

任务结果:

包含检查成功率,风险检查项,不合格主机数。

- 检查成功率:所有检查项均成功检查的主机数/总检查主机数;
- 风险检查项:风险项/总检查项;
- 不合格主机数:风险主机数/全部主机数。



检查结果概览:

• 检查策略名称检索:

■ 可输入检查策略名称进行检索,支持模糊匹配,并允许基于输入在下方联想。
 ● 仅显示风险结果开关:

- 若开启, 检查结果概览页下, 仅显示检查结果为不合格的检查策略;
- 若关闭,检查结果概览页下,显示全部下发的检查策略。
- 内容展示:
 - 检查策略:
 - ◆ 显示检查策略名称,如 CIS_level2_CentOS6/7 安全核查。
 - 核查结果:
 - ◆ 合格: 该检查策略下的所有检查项,所有检查项均为安全,则为安全;
 - ◆ 不合格: 该检查策略下的所有检查项, 存在不合格检查结果;
 - ◆ 未知: 该检查策略下的所有检查项, 不存在不合格的检查项, 且存在未知

的检查项包括 error。

- 启用检查项数:
 - ◆ 该策略的检查项数总和数量统计。
- 风险项:
 - ◆ 不合格的检查项,分别展示严重、高危、中危、低危的检查项数量。
- 风险服务器:
 - ◆ 存在风险服务器的主机数。
- 进行操作:
 - ◆ 风险项:可跳转到"风险项情况"页,附带选中的检查策略为筛选条件;
 - ◆ 风险主机:跳转到"风险主机情况"页,附带选中的检查策略为筛选条件。

2. 黄芩:	显示风险结果						
全直領略	检查结果	检查项总数	RA	21 3		风始服务器	操作
IS CentOS 7 Level 2	不合格	33 期	10		10	1台	风险项 风险主机

风险项情况:

- 检查策略名称检索
 - 可输入检查策略名称进行检索,支持模糊匹配,并允许基于输入在下方联想。
- 仅显示风险结果开关
 - 若开启,检查结果概览页下,仅显示检查结果为不合格的检查项;
 - 若关闭,检查结果概览页下,显示全部下发的检查项。
- 内容展示
 - 检查项名称:展示具体单个检查项的名称。
 - 检查策略:展示该检查项所属的检查策略。
 - 风险等级:展示具体单个检查项的风险等级,若为原先扫描出来,但当前不存在的风险检查项,风险等级以低危展示。
 - 检查类别:展示检查项的检查类别



- 风险项检查结果
 - ◆ 该检查项下,若所有的主机检查结果均为合格,则判定检查项聚合结果为 合格;
 - ◆ 该检查项下, 若存在不合格的检查结果, 则判定检查项聚合结果为未通过;
 - ◆ 该检查项下,若不存在不合格的检查结果,且存在未知的检查项,则判定 检查项聚合结果为未知。
- 进行操作
 - ◆ 点击"检查项详情"后出现弹窗,包含:
 - 描述
 - 类型
 - 验证方法
 - 修复建议
- 检查项聚合结果为未通过时,点击对应行显示影响主机。

检查结果模览 风险项情况 风险主机情况 检查策略: 请输入检查预断名称 9. 🛃 仅显示风险结果 检查项名称 检查策略 风险等级 检查类别 检查结果 操作 $\left| \cdot \right|$ 确保audt配置不可被更改 CIS CentOS 7 Level 2 我很 日志与审计 不合格 检查项详细 4 确保 /home 分区存在 CIS CentOS 7 Level 2 书化 初始化设置 不合格 10.00101210 确保 SELinux 状态是 enforcing CIS CentOS 7 Level 2 初始化设置 不合格 检查项详情 310 确保 /tmp 分区存在 CIS CentOS 7 Level 2 我准 初始化设置 不合格 检查项详情 11.2 确保 user/group 修改信息事件被... CIS CentOS 7 Level 2 日志与审计 不合格 检查项证情 4 CIS CentOS 7 Level 2 4 确保 /van/log 分区存在 任他 初始化设置 不合格 确保 /var 分区存在 CIS CentOS 7 Level 2 岳杰 初始化设置 不合格 检查项详情 + 确保启用在 auditd 之前启动的过… CIS CentOS 7 Level 2 垂泡. 日志与审计 不合格 检查项详情 + 确保在审核日志已满时禁用系统 CIS CentOS 7 Level 2 日志与审计 1578 不合格 检查项详情 确保在引导加载程序配置中没有... CIS CentOS 7 Level 2 -946 初始化设置 不合格 检查项详情 4

< 1 2 3 > 10·奈/页> 跳至 页

检查项详情	×
確保audit記量不可被更改 <mark>组织</mark>	
检查项描述	
设置系统审核,以使审核规则不能使用auditctl进行修改。 设置标志"-e	
2*会强制将审核量于不可变模式。 审核更改只能在系统重启后生效。	
检查项类型	
日志与审计	
验证方法	
运行下面命令并确认输出是否匹配:	
<pre># grep "^\s*[^#]" /etc/audit/audit.rules tail - -e 2</pre>	
修复建议	
把下面一行加到/etc/audit/audit.rules文件最后。	
-e 2	

风险主机情况:

● 检查策略名称检索



- 可输入检查策略名称进行检索,支持模糊匹配,并允许基于输入在下方联想。
- 仅显示风险结果开关
 - 若开启,检查结果概览页下,仅显示存在风险检查项的主机列表;
 - 若关闭,检查结果概览页下,显示全部的主机列表。
- 内容展示:
 - 直接展示所有主机列表,不会受筛选而遭受影响。
 - 主机地址: IP 地址
 - 主机风险情况:分别展示严重、高危、中危、低危的风险数量。
 - 检查项成功/失败:主机检查情况,展示成功项数量/失败项数量:
 - ◆ 成功项数量 = 通过 + 未通过的检查项数量;
 - ◆ 失败项数量 = 未知 + error 的检查项数量。
 - 主机检查项详细列表:
 - ◆ 检查项名称
 - ◆ 检查策略
 - ◆ 风险等级
 - ◆ 检查结果
 - 通过:检查项执行成功且判定结果为通过,显示为绿色;
 - 未通过:检查项执行成功且判定结果为未通过,显示为红色;
 - 未知:标识该检查项执行失败,存在以下情况:
 - 该检查项执行失败,返回为 error,鼠标悬浮显示对应

error_message;

■ 该检查项执行失败,鼠标悬浮 message 显示"由于网络或其他未

知原因,当前检查返回为空,建议重新检查"。

◆ 操作: 点击"检查项详情"可查看对应内容。

检查结	果瓶苋 风险项情况	风险主机情况			
检查策略	· 请银入检查然结名称 Q 2	仅显示风险结果			
	10.9.32.175	0 0 0 🚥		检查项成功/失败: 33/0	
	检查项名称	检查策略	风险等级	检查结果	操作
	确保audit配置不可被更改	CIS CentOS 7 Level 2	6.0	不合格	检察项评制
	確保 /home 分区存在	CIS CentOS 7 Level 2	(2.8)	不合格	检查运行中国
	確保 SELinux 状态是 enforcing	CIS CentOS 7 Level 2	633	不合格	检查项详细
	磯保 /tmp 分区存在	CIS CentOS 7 Level 2	(E.C.	不合格	检查项详细
	确保 user/group 修改信息事件被收集	CIS CentOS 7 Level 2	6.6	不合格	检察明详细
	确保 Avar/log 分区存在	CIS CentOS 7 Level 2	6.8	不合格	检查资详编

离线检查操作:

说明:离线检查类型任务启动后,系统会生成对应的配置文件,需要管理员下载配 置文件和检查工具在目标主机上手动执行

- 管理员需按照离线检查操作页中提示的步骤进行操作,具体操作步骤如下:
 - 下载下方的离线检查工具和配置文件,其中:
 - ◆ baseline_tool_ 开头的工具为离线批量检查工具, Windows 系统选择
 basel ine_tool_windows, Linux 系统选择 baseline_tool_linux, macOS
 系统选择 baseline_tool_darwin。
 - ◆ baseline_checker_ 开头的工具为离线单机检查工具,本次任务不需要关心, 但是必须存在
 - ◆ config.json 为在洞鉴网页上下载的配置文件文件名
 - 根据执行检查的机器的操作系统,运行检查命令

ssh_check --config --json_output

- ◆ 具体到操作系统上,以 output.json 为输出路径的话,示例如下:
- ◆ Windows 系统上,在 cmd.exe 或者 PowerShell 中运行检查工具
- baseline_tool_windows.exe ssh_check --config config.json
 --json_output output.json
- ◆ Linux 系统上,在终端中运行检查工具:./baseline_tool_linux ssh_check --config config.json -- json_output output.json
- ◆ macOS 系统上,在终端中运行检查工具:./baseline_tool_darwin ssh_check --config config.json -- json_output output.json
- 将检查结果输出文件 output.json, 在下方"导入结果"处上传, 即可查看 检查结果。



-	检查项目 资产利用	
和意味 14	cis,windows,server,2012,level_2	
检查工具下程	前往基地检查全局配置下载	
极人检查结束	支持文件格式:json 文件或多个 json 文件的 zp 包	
	B	
	点击或将文件拖拽到这里上传 文师大小平超过 100 M	
展作 80 月	1. 下载下方的高线检查工具相能要文件。其中:-	
	 baseline_checker_ 并外的工具为离析 	約检查工具、其他文件本次任务不需要关心
	2. 根据被检查的机器的操作系统,运行以下命令	
	工具文件名 check set_id 检查语 1d	ocal —host 被检查的机器 IP —json_output 输出文件各
	具体到操作系统上,以 output.json 为输出路	、 检查項 ki 请见上方的检查项 ki 碟、 以 _ cis_ubuntu_16.04_level_1 . 为例、 你例如下:
	Linux 系统上。在终端中运行检查工具	
	./baseline_checker_linux check —se	id cis_ubuntu_16.04_level_1localhost 1.1.1.1json_output output.json


3.2.2.2 进行操作

点击任务详情页面右上角的按钮,可以对任务进行一系列的操作。

编辑检查任务

- 在任务详情页可以修改扫描任务的参数配置,具体操作如下:
 - 点击右上角的"编辑扫描任务"
 - 进入编辑任务页面,修改任务的参数配置
 - ◆ 编辑扫描任务的方法与添加扫描任务基本相同,除了任务目标,基线模式, 检查策略不可编辑
 - 配置完成后,点击"保存任务"后,任务数据会自动刷新,但不会自动进行检查

立即检查

- 在任务详情页,点击详情右上角 "立即扫描" 即可启动任务
- 如果此时任务详情展示的是历史的扫描结果,任务启动时,会按照该扫描历史的参数配置来启动任务
 - 启动后,任务可能立即开始扫描,也可能进入等待扫描。这取决于系统当前正 在扫描的任务数量,是否达到了系统的最大任务并发数

停止扫描

任务正在检查或着等待检查时,若希望停止扫描或取消等待检查,可以点击右上角的"停止检查"



dd	任务	风险评级		任务进度	<u>(†</u>)	a握表 编辑检查任务 立即检查
C	高編	<mark>危</mark> 核蛮任务已发现多个不安全配置现 利用这些调调,给您造成业务损失	1, 累计评分小于等于 85 分,还意用户可能 :	已检查内容: 159 / 159		100% ∂≉⊄
任务基本配置				任务结果		
伯課人	admin	创建时间	2021-12-03	检查成功率	风险检查项	不合格主机数
执行方式	不定时扫描	结束时间	2021-12-03	1/1	65 / 159	1/1
任务类型	在线检查	运行时长	00:00:53	5645 S		
检查结束概义	风险项情况	风险主机情况				
检查策略:「這這入	10111111111111111111111111111111111111	2 仅显示风险结果				
检查策略		检查结果	F. 检查项总数 风险项		风险服务器	操作
CIS Ubuntu 18.0-	Level 1	不合緒	159 35 🔲 🚺		1台	风险项 风险主机
						< 1 > 10条/页∨

任务基本信息	
*任务名称	dd
*检查目标	
	25.25.205.57
优先级	高中低
任务速度	慢速模式 快速模式 控制基纸任务并发的速度。快速模式支持并发 50 台主机
任务速度 • 执行类型	慢速模式 快速模式 控制基线任务并发的速度。快速模式支持并发 50 台主机 不定时扫描
任务速度 * 执行类型 指定时间段	 慢速模式 快速模式 控制基线任务并发的速度、快速模式支持并发 50 台主机 不定时扫描 記給时间 ○ 至 抗束时间 ○
任务速度 * 执行类型 指定时间段	慢速模式 快速模式 控制基础任务并发的速度。快速模式支持并发 50 台主机 不定时扫描 記給时间 ③ 凝血和定时间段
任务速度 "执行类型 指定时间段 基线参数配置	慢速模式 快速模式 控制基线任务并发的速度、快速模式支持并发 50 台主机 不定时扫描 記給时间 ③ 運給的时间 ③ 運動商業时间段
任务速度 - 执行类型 指定时间段 基线参数配置 基线模式	 慢速模式 (快速模式) 控制器纸任务并发的速度。快速模式支持并发 50 台主机 不定时扫描 起始时间 ○ 至 低束时间 ○ 凝加固定时间段 在线检查
任务速度 *执行类型 指定时间段 基线参数配置 基线模式	 慢速模式 快速模式 控制器线任务并发的速度、快速模式支持并发 50 台主机 不定时扫描 副加助定时间径 查 结束时间 ○ 至 结束时间 查 结束时间 在线检查 在线检查可支持通过远程连接协议、如 ssh、对目标设备的样关文件进行读取、捕获不安全基线起置信息



3.2.3 添加基线任务

在基线任务列表界面,点击"+添加检查任务",进入添加基线检查任务的入口:

R组织中位 默认工作区 ×) + 添加等选条件 已选择 0 个任务 素能适中的任务 执行适中的任务 像止该中的任务					+ 351040300
检查任务名称	检查策略	扫描计划	检查结果	任务状态	操作
] dd	CIS Ubuntu 18.04 Level 1	无	65/159/159	◎ 已完成	10.01 8078 1618
4월 2010年3	CIS CentOS 7 Level 2	无	21/33/33	○ 已完成	HOLE BELLE SEVE
47.98.235.124	CIS Ubuntu 16.04 Level 2	无	0/0/33	◎ 已完成	1220 0039 5610
6545345	CIS Ubuntu 16.04 Level 1	无	0/0/155	② 已完成	1220 8070 5610
				121	1 2 10 条/页

3.2.3.1 任务配置

点击右上方"添加基线检查任务"按钮,出现基线检查任务配置的抽屉界面:

任务基本信息	
*任务名称	
*检查目标	手动输入 上传目标文件
	检查目标格式,以回车换行分隔: 1.1.1.1 1.1.1.1/24 1.1.1.1-255
	www.website.com 2001:0db8:3o4d:0015:0000:0000:1a2f:1a2b
优先级	高中低
17 A 12 A	400 Yan 400+ 4+ Yan 400
壮穷速度	度速模式 [状速模式] 控制基线任务并发的速度,快速模式支持并发 50 台主机
任务速度 *执行类型	1 2 2 4 4 7 1 7 12 6 7 1 1 1 2 2 4 7 1 2 5 0 台主机 控制基线任务并发的速度,快速模式支持并发 50 台主机 不定时扫描
社务速度 *执行类型 指定时间段	(夏丞候五 下冠(京五) 控制基线任务并发的速度,快速模式支持并发 50 台主机 不定时扫描 和政治时间 ○ 至 55 束时间 ○
任务速度 •执行类型 指定时间段	國法保入 K法保入 控制基线任务并发的速度,快速模式支持并发 50 台主机 不定时扫描 起始时间 ③ 至 结束时间 ③ 蒸加描述时间段
任务速度 *执行类型 指定时间段 基线参数配置	國法保入 K送保入 控制基线任务并发的速度,快速模式支持并发 50 台主机 不定时扫描 超始时间 ③ 五加时间 ③ 五加市定时间段
任务速度 • 执行类型 指定时间段 基线参数配置 基线模式	★ 2 (大法何天) 控制基线任务并发的速度,快速模式支持并发 50 台主机 不定时扫描 和室町扫描 超始时间 ③ 至 第次時定时间段
任务速度 *执行类型 指定时间段 基线参数配置 基线模式	 ★ 1 ★ 1 ★ 1 ★ 1 ★ 1 ★ 1 ★ 1 ★ 1 ★ 1 ★ 1
任势速度 * 执行类型 指定时间段 基线參数配置 基线模式 检查策略	國本報末 KEGK 控制基线任务并发的速度,快速模式支持并发 50 台主机 不定时扫描 起始时间 ③ 至 结束时间 返加指定时间段 在线检查 在线检查 在线检查 在线检查 在线检查 在线检查 有线远程基线检查可支持通过远程连接协议,如 sah,对目标设备的 关文件进行读取,捕获不安全基线配置信息 请输入关键词检索



进入任务配置页面,设置任务的基本信息和基线参数配置

3.2.3.2 任务基本信息参数

任务名称(必填项):

● 对该任务进行命名标识

任务目标(必填项):

- 手动输入 按照提示的格式输入目标地址
- 文件上传 下载文件模板进行填充后上传,可用于批量站点的任务下发
 - 若选择文件上传方式,则无需填写下方基线参数配置的登陆方式等参数:



优先级(必填项):

- 执行时被引擎扫描的优先级
- 可选择高优先级、中优先级、低优先级三种,默认为中优先级

任务速度(必填项):

- 快速模式:支持并发 50 台主机;
- 低速模式:支持并发 20 台主机;
- 默认为快速模式,最大并发主机数越高,扫描速度越快,性能消耗越强。

执行方式(必填项):

- 立即扫描
- 定时扫描一次



- 每天循环扫描
- 每周循环扫描
- 每月循环扫描

指定时间段(必填项):

 通过指定相应时间段控制任务的执行时间,当任务在指定时间段内未完成时将进入 暂停状态,下次到达后将进行断点续扫。

3.2.3.3 基线参数配置

基线模式(必填)

分为"在线远程基线检查"、"离线本地基线检查"、"离线批量基线检查"三种模式

- 在线远程基线检查——在线远程基线检查可支持通过远程连接协议,如
 ssh,对目标设备的相关文件进行读取,捕获不安全基线配置信息
- 离线本地基线检查——离线本地基线检查可支持通过本地程序运行的方式,对当前文件所在设备的配置进行读取,捕获不安全基线配置信息
- 离线批量基线检查——离线批量基线检查可支持通过生成配置文件和本地
 程序的方式,依赖堡垒机等介质设备对目标进行检查

检查策略(必填)

- 可以选择多个基线检查策略执行
- 支持按策略名称、检查对象、所属标准检索
- 支持跨检查对象类,勾选基线检查策略
- 策略受基线模式影响,对应模式将影响策略列表的加载
- 当选择 MySQL 和 PostgreSQL 两种数据库策略且数据库宿主机不开启

SSH 服务时,需要在目标主机中添加跳板机。为不影响检查结果,最好不要将数据库策略和其他策略混选。



当选择 MySQL 和 PS 数据库策略且数据库存 SSH 服务时,需要在 1 跳板机。为不影响检查 要将数据库策略和其他	程主机不开启 目标主机中添加 ■可支持通过远程连接协议,如 ssh,对目标设备的 短年,最好不可义,捕获不安全基线配置信息 3策略混选。
检查策略 ⑦	请输入关键词检索
	▶ 操作系统安全合规
	▶ 常规中间件安全合规
数据库配置参数	▶ 虚拟化容器安全合规
	▼ 数据库安全合规
	CIS标准 PostgreSQL Level 1
	CIS标准 MySQL Level 1
	CIS标准 MongoDB 3.6 Level 1

数据库配置参数(非必填项):

 选择数据库 Mysql 和 PostgreSQL 数据库类策略必填,多种数据库参数可换行 分隔,输入参数需要匹配对应的数据库配置格式。

登陆方式: 必选, 支持 SSH 或 SMB 的方式

- SSH
 - SSH 端口(必填项)
 - SSH 用户名(必填项)
 - SSH 认证口令(必填项)
 - SSH 服务登录认证口令, 分统一密码、SSH 私钥、两种类型
- SMB
 - SMB 端口(必填)
 - SMB 用户名(必填)
 - SMB 密码(必填)

任务执行



检查参数无误后,点击右下角的"仅创建任务"按钮或"创建并立即扫描任务",即可 创建任务。

	在线检查					
	在线远程基线检查可支持通过远程连接协议。如 ssh,对目标设备的相关文件 进行读取,捕获不安全基线配置信息					
检查策略 ③	③ 请输入关键词检索					
	被选择的基线策略包含的所有检查项均会被用于在任务目标里执行,选择错误 的基线策略可能影响评估结果的准确性					
数据库配置参数	选择数据库类策略必填。多种数据库参数之间可以换行分隔,输入参数需 要匹配对函数据库约配置格式,样例如下: MYSQL 样例: 'user:password@addr[:3306][?dbname]' POSTGRES 样例: 'postgres://user:password@addr[:5432]/dbname? sslmode=disable' oracle 样例: 'oracle://user:password@addr[:1521]/[dbname]? ssl=false&dba privilege=sysdba'					
登录协议	SSH v					
	22					
*SSH 服务端口						
* SSH 服务端口 * SSH 登录用户名						
* SSH 服务端口 * SSH 登录用户名 * SSH 登录认证口令	统一密码 SSH 私钥					



3.2.4 基线检查配置

在左侧导航栏中,选择"基线管理-基线检查配置",进入基线检查配置界面。

<->洞鉴x-	RAY			admin
默认工作区	M	- - - - - - - - - - - - - - - - - - -		
 ・	* 4	88H 认证私钥配置 此处私钥向于基线检 6	1回时 with 登ូ接密钥以证方式 3原因时间 2021-12-03 11:23-12 ■m	
基林检查配置		真线基线检查工具下载	AB-74H	
冬 資产中心	*	操作说明	1. 创建潮场检查任务	
* #822	×		2. 下粮检查工具	
圓 报表中心	×		3. 在对应黑线检查任务评师几下载配置文件邮本	
2 10 F/R	÷		4.在检查机器上运行版本	
③ 系统管理	*		5. 检查兜试后回传,在下方上传文件	
△ 均户按理	сų	检查工具下载	检查工具版本: 2.0.10	
			ASTER	

3.2.4.1 SSH 认证私钥配置

此处私钥用于基线检查时 ssh 登录密钥认证方式(如下图),通过添加私钥名称 和 SSH 私钥,点击确认添加证明。

加 SSH 认证私	钥
* 私钥名称	请填写,该名称作为任务配置时的显示标识
* SSH 私钥	请输入认证私钥
	取消 确 完



3.2.4.2 离线基线检查工具下载

包含操作说明,以及检查工具的版本信息和下载入口,点击进行下载

离线基线检查工具下载

操作说明

- 1. 创建离线检查任务
 - 2. 下载检查工具
 - 3. 在对应离线检查任务详情页下载配置文件脚本
 - 4. 在检查机器上运行脚本
 - 5. 检查完成后回传,在下方上传文件

检查工具下载

检查工具版本: 2.0.10





3.3 镜像管理

在左侧导航栏中,选择"基线管理-基线检查任务列表",进入基线检查任务列表界面。

<・> 洞豐x	RAY								admin
默认工作区	×	1億日間 / 镀像扫描任务列表							
② 全局仪表盘		新展组织单位 數认工作区 ×	+ 添加等选机	t/#					
日 扫描管理	,	已选择 0 个任务					自动照新 👩	○ 批量操作 ~	+ 源加扫描任务
A 基线管理	~	任务名称	目標类型	创建用户	所属组织单位	风险结果	任务状态	最近扫描时间	创建时间
品 積像扫描	^				0.000		11121112		
關保曰擔任务列表									
念 资产中心	×					Del.			
△ 漏彩管理	¥					96.7540.85			
盲 报表中心	~							#08	10.50
🖾 幼识期	¥							AVR COU	10.38/30.5
④ 系統管理	~				X-Ray XR-S(H) 10	1-24.06.001_r11 @ 2024 Chailin Ted	n.		
☆ 用戶管理	2								

3.3.1 镜像扫描任务列表

展示创建的镜像扫描列表,包含"任务名称"、"目标类型"、"创建用户"、"所属组织 单位"、"风险结果"、"任务状态"、"最近扫描时间"、"创建时间"

支持对"所属组织单位"、"任务名称"、"任务状态"、"创建时间"、"最近扫描时间"进 行筛选

支持对镜像扫描任务批量执行"删除"、"启动"、"停止"操作



3.3.2 添加镜像扫描任务

3.3.2.1 镜像文件

< → 洞盟x-						
默认工作区	~	1.11日回 / 镇像扫描任务判决	添加任务			(x)
※ 全局仪表盘		(M型田田市市 就以工作区 ×) + 漆加菁选条件				
	c	● E选择 0 个任务	* 任务名称			
4 基场管理	×	石木之论 目标并可 何律而户 新聞的印象的 副	* 扫描目标	镜像文件	远程仓库	
A 玩像日道	-					
就像目前任务列队					1	
● 田戸中心	~	1- <u>1-</u>			点击或将文件	牛拖拽到这里上传
◎ 兼約管理		NAR.		说明:对上传	的镇像文件进行风险	探测:同时支持一个镇像文件的扫描
G 报表中心	~					
C seam	6					
③ 系统管理	~	# Hay 201-8(H 10-24.08.001)				
△ 用戶管理						
					取消仅	创建任务 创建并立即扫描任务

支持上传".tar"格式的镜像文件,作为扫描目标

导出镜像的方式:

- 1. 找到要导出的镜像全名称(格式 registry/[path/]image[:tag])
 - (1) repository: 仓库名,通常是一个用户名或者组织名。
 - (2) path: 路径名, 通常用于区分业务
 - (3) image: 镜像名称
 - (4) tag: 标签, 默认为 latest

2. 执行导出命令:

- (1) docker save -o nginx.tar 10.9.34.84:5000/nginx:latest
- 注:导出镜像 Tag 时,不能使用 tag 的 ID



3.3.2.2 远程仓库

< →洞溫 _{x-r}	RAY			admin
默认工作区	×	1995年1月/ · 镇像扫描任务列表	添加任务	x
© 全局仪表盘		(MMARRING 就以工作区 ×) + 液加器送条件		
23 扫描板理	e.	● B遠祥 0 个任务	* 任务名称	
J 基场管理	×		* 扫描目标	镇像文件 远程仓库
华·铁维白道	4			说胡:通过访问远程仓库的方式获取目标锁像并进行风险探测;支持 多个目标锁像的扫描
地像目前任务学校			* 仓库类型	DOCKER_REGISTRY_V2
● 初戸中心			• A #1414	
☆ 東府新規		12.0	- 日神明年	
第 报表中心	~		* 置名访问	
囗 蛇病病	3		* 用户名	
③ 系统管理	×	8-Rey XR-8(-9) 10-24.08.001		
△ 用戶審理			* Token	
			* 目标镜像	获取镜编
				取 消 仅创建任务 创建并立即扫描任务

通过远程登录镜像仓库上,获取镜像目标,进行扫描

注: 该版本仅支持 DOCKER_REGISTAR_V2 的仓库类型

需要配置仓库地址、用户名、token,支持匿名访问

正确配置完上述信息后,点击"获取镜像"

在弹窗中选择,需要扫描的镜像文件

注: 该版本每个镜像只获取其中一个版本, 默认为 latest, 当不存在 latest 则获取 列表最后一个镜像

3.3.3 镜像扫描任务详情

3.3.3.1 任务信息

当扫描任务正在扫描中时,展示进度条,当扫描结束后,隐藏展示

展示漏洞数量分布图

展示任务基本信息。包含扫描状态、扫描目标类型、启动时间、扫描时间



								admin
×	请你扫描 / 模像扫描任务列表 /	镜像扫描任务详情						
	任务详情 / 匿名修改者	名称					编辑任务	立即扫描
Ŷ	任务信息 漏洞 (1083)	销像 (5)						
×								
^	漏洞数量				任务基本信息			
					扫描状态	已完成		
×			• 严重	125	扫描目标	远程仓库		
¥			高危	501	启动时间	2024-05-25 15:13:37		
×			• 低危	50	扫描时间	00:01:10		
~								
~								
			X-Ray XR-SP	010-24.08.001.711 0.20	24 Chailin Tech.			
		 株舗用料/ 植像田園住秀和美/ 任务详情/ 匿名修改: 任务详情/ 匿名修改: (15/16) 第時(1083) 第時間数量 	* 株単日油 / 桃像白脂在多羽菜 / 植像日脂在多羽菜 / 植像白脂在多羽菜 / 植参白脂在多羽菜 / 植参加 * 日本 / 枝 / 図名修改名称 * 日本 / 枝 / 図名修改名称 * 日本 / 枝 / 図名(*003) * 田本 / 枝 / 図 * 田本 / 枝 / 図	・ ・	● 秋田田川 / 桃田田田子奈明美 / 桃田田田子奈祥博 日务详情 / 図名修改名称 近方信息 第月 (1083) 現像 [5] 調閲数量 ● 小戸重 125 和政数 ● 小戸重 125 和政数 ● 小売 407 ● 低意 501 ● 北市 407 ● 松売 407 ● 松売 501 ● 米田 50 ● 米田 50	● RefEild / 現像目間任务列表 / 機像目間任务列表 任务详情 / 匿名修改名称 ● 日本 ● 日本 ■ 調放量 任务基本信息 ● 严重 125 日期状态 ● 严重 125 日期目标 ● 作意 407 日期到间 ● 化色 50 日期引向 ● 化色 50 日期日前	● Referite / 機像自器任务分核 任务详情 / 匿名修改名称 「日务行業 / 尾名修改名称 日本 「日务行業 / 第7(003) 後集(5) 日本 編測数量 日本 ● 戸重 125 日田市振 送屋仓库 ● 花 407 日田市県 送屋仓库 ● 花 407 日田市県 ご和 0091:10	● RateH / 構像目描任务7時/ 使用目描示的特殊 日分算情 / 医名修改名称 新報 (1003) 制像 (5) ● 原類 日報応応 日報応応 日報応応 ● 原類 125 日期目标 話程台集 ● 作質 125 日期目标 話程台集 ● 作意 407 日期时 000110 ● 化合 407 日期时 000110 ● 化合 407 日期时 000110

3.3.3.2 漏洞列表

展示镜像扫描版本匹配到的漏洞列表,包含"漏洞等级"、"漏洞名称"、"影响目标" 字段

<・> 洞鉴x-	RAY						admin
默认工作区	×	領急目前 / 観像扫描日	E务列表 / 镜	像扫描任务	译情		
© 全局仪表盘		任务详情 / 匿:	名修改名称	称			编辑任务 双联扫描
日 扫描管理	¥	(58/17)	91 (1083)	(第49-(5)			
A 基场管理	*	12.25118-65	in (roost	100 Her (0)			
高 铁像扫描	~	潮洞帶班:			漏洞名桿:		23 12
随像扫描任务列表		漏洞等级			漏洞名称	影响目标	操作
念 资产中心	~	-			CVE-2023-6992: zilb 緩冲区错误漏洞	10.9.32.177:5000/centos:latest	全相详细
△ 混彩管理	÷	-			CVE-2022-37434; zlib 缓冲区错误漏洞	10.9.32.177:5000/centos:latest	8.8.17M
亩 报表中心	~	-			CVE-2018-25032: zlib 缓冲区错误漏洞	10.9.32.177:5000/centos:latest	皇香祥储
口 知识库	×				CVE-2023-45853: zlib 输入验证错误源词	10.9.32.177:5000/centos:latest	里板详统
② 系統管理	*	-			CVE-2021-32803: node-tar 后置链接漏洞	10.9.32.177:5000/centos:latest	度最详细
☆ 用户管理	3				CVE-2021-32804; node-tar 路径遍历淵洞	10.9.32.177:5000/centos:latest	皇影评情
		-			CVE-2021-20193: git tar.git 安全漏洞	10.9.32.177:5000/centos:latest	遊園洋橋
		88			CVE-2019-9923: GNU Tar 代码问题源词	10.9.32.177:5000/centos:latest	查斯详慎
					CVE-2022-48303: GNU Tar 銀冲区错误漏洞	10.9.32.177:5000/centos:latest	酒着详细

支持根据"漏洞等级"、"漏洞名称"进行筛选

点击"查看详情",可在弹窗中查看漏洞描述和漏洞修复方案等信息



< → 洞豐 x-			漏测详情	×	admin
默认工作区	×	10月1日)/ 秋 像白褐任务列	CVE-2023-6992: zlib 缓冲区错误漏洞		
© 全務仅表盘 円 臼根繁珠	c	任务详情/匿名修	国府相逆 zib是美国Mark Adler个人开发者的一个通用的数据压缩库。zib-存在安全漏洞,该漏洞跟于存在缓冲区溢出 赢用,导致defato.c比现内存损坏。		編編任务 立即扫描
▲ 基场管理 ▲ 積量扫描 簡単日間任务700	•	派羽驾迎: 潮羽等级	里对编号 CT-1032543 CVE-7023-6992 CNWVD-202401-257		● 第 ■ ■ 級作
● 表产中心	÷	633	漏消被踢时间		
○ 東京教理			2024-01-04 00:00:00 演用品書 可能派成這点信息逆篇, 业务系统不稳定等安全问题		
C 10.00	5		CVSS 风险评分 5.5		
② 系统管理	~	-	形 時候作 a color differenzib		2019
- m/ ma			影响范围 zilo<2023-11-16		会新订 物
			点击查看影响范围详情 终复方案 建议反映编复安全问题,并做好安全管理工作。定期进行安全派给。最大程度地源免安全问题。		· · · · · · · · · · · · · · · · · · ·
		E03			561718

3.3.3.3 镜像列表

展示镜像扫描识别到的镜像列表,包含"镜像名称"、"风险结果"字段

<・> 洞甇 _{X-F}	AY			sdmin
默认工作区	×	项俳曰地 / 镀像扫描任务列表 / 镀像扫描任务详情		
② 全局仪表盘		任务详情 / 匿名修改名称		编辑任务 立即归籍
日 扫描管理	2	任务信息 漏洞 (1083) 镜像 (5)		
』 基线管理	*	· · · · · · · · · · · · · · · · · · ·		0.00 R 97
為·積優扫描	^			
續像目擔任务列表		镜像名称	风险结果	操作
念 责产中心	×	10.9.32.177:5000/centos:latest	27 105 20 0	8 (File)
☆ 混彩管理	¥	10.9.32.177:5000/registry:2.7.0	6 60 6 6	<u> </u>
亩 报表中心	v	10.9.32.177:5000/link:10-24.04.001_r7	22 🐻 📴 👩	D Sizeria Sizeria
🖾 Mirm	٧	10.9.32.177:5000/gungnir:6.15.5_r1	61 📾 💷 🛤	2. 空間評問
② 系统管理	*	10.9.32.177:5000/nginx:1.19.0		查看详情
☆ 用戶管理	2			共5条 < 1 > 10条/页 >
			X-Ray XH-S(H)	19-24.06.001_r11 0 2024 Dialtin Tech.

支持通过镜像名称进行模糊匹配

点击"查看详情", 跳转查看镜像的应用信息和关联的漏洞信息

应用信息展示识别到的应用列表,包含"应用名称"、"应用版本"字段



<・> 洞甇x-i	RAY			admin
默认工作区	×	真你目绌 / 镀像扫描任务列表 / 镀像扫描任务译情 / 扫描详情 / 镜像详情		
② 全局仪表盘		镜像详情 / 10.9.32.177:5000/centos:latest		
日 扫描管理	3	应用信息 漏洞信息		
.4 基线管理	~			_
品 镀像扫描	^	臣用名相	应用版本	_
输像扫描任务列表		złb	12.11	
念 责产中心	×	yum	4.4.2	
☆ 還將管理	v	xz-liba	5.2,4	
亩 报表中心	~	xz	5.2.4	
C 知识库	Ŷ	vim-minimal	8.0.1763	
◎ 系統管理	v	util-linux	2.32.1	
☆ 用戶管理	v	tzdata	2021a	
		tpm2-tss	2.3.2	
		tar	1.30	
		systemd-udev	239	

3.4 资产中心

此模块主要用于企业的资产进行管理,系统将企业的资产数据进行综合统计计算 并可视化,方便直观的展示给用户,并支持对已知资产与未知资产进行集中管理,包括 对资产的查询、筛选、添加、删除、快速扫描等操作。企业可对资产进行分组和指派责 任人、管理员。

3.4.1 资产全景

在左侧导航栏中,选择"资产中心-资产全景",进入基线检查配置界面。

此页面针对资产数据进行综合统计计算,生成可视化数据直观展示用户在资产管理场景下需要的数据,便于清楚当前所管理的资产情况,支持筛选查找和清空缓存。



3.4.1.1 内容展示

资产概览:

- 此处展示当前用户在系统中的资产管理关键指标及资产的地理位置分布;
- 展示的信息包括:
 - 资产总数,主机资产数,Web资产数,未知风险资产(未做过安全检测的资产),
 不存活主机资产数(仅针对主机资产)及资产的地理位置分布。





资产运行情况:

- 此处展示当前用户在系统中各个资产的运行情况统计数据;
- 环状图展示主机资产的运行情况占比, 鼠标悬浮在环状图上会出现相应的运行状态 数量及占比。

资产风险等级分布:

- 此处展示当前用户在系统中资产的风险等级统计数据;
- 环状图展示资产的风险等级,鼠标悬浮在环状图上会出现资产的风险等级数量及占比

资产指纹画像:

- 此处展示当前用户在系统中的资产指纹的相关统计数据;
- 展示的信息包括:
 - 开放端口的资产占比及排名
 - 服务程序的资产占比及排名
 - 应用中间件的资产占比及排名
 - 设备类型的资产占比及排名
 - 操作系统的资产占比及排名
 - CMS 系统的资产占比及排名
 - 使用语言的资产占比及排名
- 点击标签可切换资产指纹;
- 鼠标悬浮在资产占比的表头上时会出现资产占比的计算公式。



在产指纹画像							
期口开放爆浪	服务程序	应用中间件	设备类型	质作系统	CMS Kitt	使用语言	
#6		,	平設端口				意产品比
5			43				11,895
2		a	0				15.496
3		2	2				9.7%
4.			45				22%
5		2	1				2.0%

业务系统资产分布:

- 此处展示当前用户在系统中资产的各业务系统使用资产的分布及排名情况;
- 展示的信息包括:
 - 左侧条状图展示业务系统资产的排名及占比
 - 右侧的表展示业务系统的排名及资产数量
- 左侧条状图基于右侧表变换数据;
- 鼠标悬浮在业务系统名字上时会出现业务系统的名字。

	③ 暫无敗端	排名	业务系统	资产数
			NAME.	
拉资产分布				<. 0
位资产分布 70 50		排名	所属组织单位	< 0 资产数
拉第产分布 30 50 30		那名 1	所属雄织单位 默认工作区	 ① ① ⑦产数 828
2.第产分布 i0 i0 i0		排名 1 2	所憲提织争位 默认工作区 就认工作区-test2.1-test2.1.1-test2.1.1.1	⑦ (1) 現代数 828 2

组织单位资产分布:

- 此处展示当前用户在系统中资产的组织单位资产分布及排名情况;
- 展示的信息包括:
 - 左侧柱状图展示组织单位的资产数量情况
 - 右侧表展示组织单位的资产数排名情况
 - 左侧柱状图图基于右侧表变换数据
- 鼠标悬浮在左侧柱状图的某项数据上会出现该组织单位的名字及资产数量;
- 鼠标悬浮在右侧表的组织单位名字上会出现该组织单位的名字。



264

50

44

119

453

52

3.4.1.2 筛选资产

在资产全景页可对资产进行数据筛选操作,以改变资产全景页展示的数据,可根据 业务系统,组织单位,所在地址,网络区域,标签进行多维度的筛选操作。具体操作为:

- 查看维度: 默认工作区 选择数据聚合组度 资产概定 资产运行情况 -831 455 376 31.8% 资产位置分布 . (0.40.4 · ** • 来北市 • 中危资/ • 安全资产 未知资产 分布数量 大量出行 Э.量资产 +50 0.0010100000
- 点击页面右上角的选择数据聚合维度:

弹出筛选条件对话框。由于数据量比较大,多维度的筛选可能会影响页面性能;

业务系统		Ÿ
组织单位	农行总部	×
所在地址	请选择	×
网络区域		Ŷ
标签		v
截止日期	2021-12-14 📋	

筛选的条件会在全景页的右上角"查看维度:xxx"展示,悬浮在维度上会出现所有筛 选的维度;





- 填写想要筛选的内容,并按下"聚合维度"按钮进行筛选;
- 想要重置筛选内容,可以点击"重置条件"按钮,清空筛选对话框的内容,再点击"聚 合维度"按钮,将筛选的资产复原。

3.4.2 主机资产

在左侧导航栏中,选择"资产中心-资产列表-主机资产列表",进入主机资产列表 界面。

<・>洞≝ _{x-}	RAY													adm	nin
默认工作区	~	<u>東</u> 严中心)	BP#	(高 / 主机资产列表)											
© 全局位表量		(HIMR	朝東位	MULTRE X) (PR	地 存活 ×) (+ 添加筛选条	1									0
日日接後期	×	0 2	选择 0	个主机					存活动	<u>نة</u>	łł	量操作 ~	十手动	i\$nu±4	机
A 基线管理	*			资产地址	内部负责人	所属组织单位	业务系统	风险等级	8 8 8				操作		
き 資产中心	*	0		10.3.0.112	admin	默认工作区		无风险			12			AM BI	8
资产全景	~	G		10.3.0.8	admin	默认工作区	- 22	有关验	8		0			A18 80	
主机资产列表			•	10.3.0.111	admin	默认工作区		无风险	.0	0	.0		9 8 8	852 BIS	
Web 粘点资产	98	10		10.3.0.7	admin	默认工作区		无风险	63	0	13		-	AM HIS	8
资产组织表		, ti		10.9.33.32	admin	默认工作区		无风险	8	13			-	615 BIT	
资产属性管理	×			10,3.0.8	hyi03	赋认工作III-hyl01-hyl02	12	元共建	63	-			28 8	ast mit	
A 漏的管理	×			10.3.0.6	hyl03	默认工作区-hyl01-hyl02		海风险	0				25 8	Rist His	
盲 报表中心	٠			10.3.0.210	hyi01	默认工作区-hyl01		无风险	0				-	A18 807	
〇 知识库	*			10.9.33.70	admin	默认工作区		无风险	0					411 BIT	
② 系统管理	×			10208	hv001	解注工作収入から1		10 M M		-		-			
△ 用户管理	÷				. nym t	and wrong the state of		(1 2	3	4 >	10 条/页	- RE		页



3.4.2.1 主机资产列表

内容展示:

主要展示所有的主机资产信息,内容包括:资产运行情况(资产地址前的圆点)、 主机资产地址、资产负责人、所属组织单位、业务系统、风险等级和各漏洞等级数量:

<・>洞鉴x-RAY	6													a	dmin
默认工作区 〜	X 10%	PØ-73	11-33	※ / 主机资产列表											
② 全局仪表盘		MIRLER	市際位	₩\J1作区 ×) (77	111 存活 ×) + 添加降选条(ŧ									\$
日相論管理		• E3	i# 0	个主机					存活动动	5.	2.5	Lilleffi 🗸	+ 手	ហរតាវទ	主机
d 基线管理	· (h.		帝产地址	内部负责人	所屬組织单位	业务系统	风险等级	漏洞数量				揚竹		
意 资产中心	. ((-	-			
语产全景			*	10.3.0.112	admin	默认工作区		无风障		100		H	24	511	HRR.
道广列表			•	10.3.0.8	admin	默认工作区		高风脸	۲	8				5611	11.12
主机资产列表	1		•	10.3.0.111	admin	默认工作区	82	无风险	0	0			26	1818	1 122
Web 站点资产列表			•	10.3.0.7	admin	默认工作区	1	无风险		8				58.91	BOR.
资产组列表				10.9.33.32	admin	默认工作区		无风险	0					-	10 100
资产属性管理	v.		•	10.3.0.8	hytoa	默认工作区-hyl01-hyl02		无风度	10	13	0	0	-	10110	10 ,88
0 週初管理	*		•	10.3.0.6	hyl03	默认工作区-hyl01-hyl02	52 E	高风险						511	単称
□ 报表中心 、	×			10.3.0.210	hyl01	默认工作区-hyl01	3	无风险	.0						B 128
口如识版	~			10.9.33.70	admin	默认工作区		2.00		12	13		20	-	
③ 系统管理	*														
△ 用户管理			•	10.3.0.6	hyl01	默认工作区-hyl01	-	无风险	0	0		8	章章	5538	BIR .
									< 1 2	3	4 >	10 条/页	展至		页

筛选主机:

在主机资产列表页可对主机资产进行筛选,可根据资产地址、风险等级、内部负责 人、外部负责人、组织单位、业务系统、标签、网络区域、操作系统、设备类型、资 产名称、所在地址、端口、应用程序、服务类型,自由添加一个或多个条件进行筛选, 具体操作说明如下:

● 点击"添加筛选条件"按钮,弹出添加筛选条件对话框;

- 选择要增加的筛选条件类型并填写相应的要筛选的内容;
- 点击"增加一个筛选条件",可以增加筛选限制条件;
- 点击"删除",可以删除掉不需要的筛选限制条件;
- 筛选条件限制至少要添加一条;
- 设置好条件后,点击"保存",即可展示符合筛选条件的列表。
- 筛选条件按照使用优先级进行排序
 - 例:选择"相关扫描任务"和"资产组名称"的筛选条件,允许用户根据

扫描任务和所在资产组名称进行多组筛选。

■ 筛选功能优化:



◆ 选择"应用程序"筛选条件,可进行应用程序版本号的批量搜索,

	添	加筛选条件				>	¢
		所属组织单位	<u> </u>				
	1	所属组织单位 内部负责人	组织单位	1不能为空			
		外部负责人 相关扫描任务 漏洞名称		STATE PER		取消保存	1
		漏洞编号 漏洞等级	nin	默认工作区		无风险	8
		漏洞状态处理	nin	默认工作区	1.	无风险	
添加筛选条件				×	添加筛选条件		×
相关扫描任务 🗸	detest ×	detail-test × asdfasd	fasd ×		資产組名称 ∨	test4 × test3 ×	
+ 酒加雜送条件	测试-默认工 detest detail-test	作区		× × 1 87	十 添加隊选条件	7777777 112234 test4	×
ac	asdfasdfas I2345	d		w l	admir	自动同步	40
at	dmir 1 日志	左左间前4-15 缺注		00	adma	test2 ip段资产组 test1-0111	
ž	和筛选条	件					×
择	应用程序	~	openssh		6; 8	模糊匹配∨	
	十 添加筛	読条件					本
•						取消	保存

不同版本之间用英文符号";"分隔。

添加主机:

在资产列表页可以通过手动添加一个或导入 cvs 文件的方式添加资产,方便管理员添加企业资产,具体操作为:

● 在列表页点击 " + 手动添加 XX 资产",显示填写内容的弹窗:



动添加主机		
手动添加	文件上传	
* 资产地址	请输入多个主机资产,支持网段输入,多个资产换行分隔示例: 10.6.12.1/24 10.6.12.1-255 10.6.12.1 10.6.12.1 2001;0db8:3c4d:0015:0000:0000:1a2f:1a2b 2001;0db8:3c4d:0015:0000:0000:1a2f:1a2b/24	le
资产名称	请输入资产名称对资产进行描述	
*所在地址	北京市 / 东城区	v
*组织单位	默认工作区	×
* 内部负责人	admin	v
外部负责人		
资产组	请选择资产组	v
*资产权重	3	v
业务系统	请选择资产所属业务系统	N.
网络区域	请选择资产所赢网络区域	y.

- 选择添加方式:
 - 手动添加一个资产
 - 上传资产文件(上传资产文件完全后,会提醒资产的上传结果)



添加资产失败可能因 必填项导致]为资产内容输入格式有误,或者没有按照规	则输,
添加失败 5 条资产,添	加成功 0 条资产,此前已经添加过 0 条资产	
添加失败的资产列表	192.23.23.34 192.23.。。23 192.5.5.5 192.5.5.5 2001:0db8:3c4d:0015:0000 :0000:1a2f:1a2b(示例)	
来源:文件上传 主机 3 添加时间: 2022-03-07	资产文件test1.csv 11:59:10	

- 按照不同方式的添加要求,填写选择资产相关信息包含(资产地址、资产名称、 所在地址、组织单位、内部负责人、外部负责人、资产组、资产权重、业务系 统、网络区域、标签);
- 点击"确定"按钮,完成资产添加。
- 注意:
 - 已经存在的资产不能被重复添加;
 - 上传文件格式必须严格按照模板提供的格式添加,不同资产列表的模板不一样,请下载查看生成主机资产报表。

生成报表:

在主机列表页可以选择多个主机并生成所选主机的报表,具体操作为:

- 选中希望生成报表的主机资产,此时显示已选择的主机资产总数,同时"批量 操作"--"生成报表"按钮变为可点击状态;
- 点击"批量操作"-"生成报表"按钮;
- 在弹出的窗口中, 输入相应的生成配置;
- 点击"确认",即可开始生成报表。可以前往报表管理页面查看报表生成的情况,或下载生成好的报表。
- 当选择超过一个主机资产时,可生成"资产对比报表"。



用单位 長择 2	BUI作区 X (存活 な) 今主机 廣产地址	+ 滚加筛选条件 内部负责人	5 1 5 1 6			存活动	态 …	Ĩ	社業操作、	+ #	ផាតិវត	٢
表择 2	今主机 资产地址	内部负责人	新聞相口動作			存活动	œ	T	社業操作 >	+ 手	រាក់វា	-
•	资产地址	内部负责人	新建物织菌作								_	主机
•	10 3 0 112		731.000 HELMEN THE 164	业务系统	风险等级	派司数			8119	操作		
	The state of the	admin	默认工作区		王风靡	.0		1	總祖	20	16.98	86.00
	10.3.0.8	admin	赋认工作区	-	高风险	3		1	导出 生成报表	26	1510	-
	10.3.0.111	admin	默认工作区		无风险				下发任务	28	1611	H 20
•	10.3.0.7	admin	默认工作区		无风险	13	0	0	8	24	5512	(K33)
•	10.9.33.32	admin	默认工作区		光风险	13	П.			24	1818	8510
•	10.3.0.8	hyl03	默认工作区-hyl01-hyl02		无风险	0	8	8		28	1610	19634
	10.3.0.6	hyl03	默认工作区-hyl01-hyl02		高风暗	.03		0		26	1811	84.39
	10.3.0.210	hyl01	默认工作区-hylD1		无风险	13				-	5618	2 (12)
	10.9.33.70	admin	赋认工作区		王风助	8	13				1618	-
	•	 10.3.3.32 10.3.0.8 10.3.0.5 10.3.0.210 10.9.33.70 	10.9.33.32 admin 10.3.0.8 hyl03 10.3.0.6 hyl03 10.3.0.210 hyl01 10.3.0.210 admin	 10.9.33.32 admin 駅以工作区 10.3.0.8 かり03 駅以工作区-hy01-hy02 10.3.0.6 かり03 駅以工作区-hy01-hy02 10.3.0.210 かり01 駅以工作区-hy101 10.8.33.70 admin 駅以工作区 	 10.9.33.32 admin 数以工作区 10.3.0.8 hyl03 数以工作区+hyl01+hyl02 10.3.0.6 hyl03 数以工作区+hyl01+hyl02 10.3.0.710 hyl01 数以工作区+hyl01 10.2.33.70 admin 数以工作区 	103.33.22 admin 取以工作区 - 系発電 103.0.3 1½03 配以工作区 - 正規電 103.0.310 1½04 配以工作区 - 正規電 103.0.370 含dmin 配以工作区 - 正規電	103.03322 admin 取以工作区 - 系ス株 回 103.04 17/03 取以工作区 - 第ス株 回 103.05 17/03 取以工作区 - 第ス株 回 103.0510 17/03 取以工作区 - 第ス株 回 103.0510 17/03 取以工作区 - 第ス株 回	103.03 面dmin< 取以工作区 - 系規数 二 103.03 hyl03 取以工作区-hyl01-hyl02 - 第規数 二 二 103.04 hyl03 取以工作区-hyl01-hyl02 - 第規数 二 二 103.05 hyl03 取以工作区-hyl01-hyl02 - 第規数 二 <	103.03322 admin 飲以工作区・+y(01++y(02) - 原業務 日 <th1< th=""> 日 日</th1<>	103.032 admin 取以工作区・hy01-hy02 - 東東市 第二日 第二日 <td>105.33.22 点 dmin 取入工作区 - 原本部 日</td> <td>105.33.32 admin 取込工作区 - 東京都 日</td>	105.33.22 点 dmin 取入工作区 - 原本部 日	105.33.32 admin 取込工作区 - 東京都 日

生成报表				×
*报表名称:	10.3.2.134、10.3.2.142等的资产	ド报表		
* 所属组织单位:	默认工作区			×.
* 报表类型:	资产对比报表			×
* 报表模板:	资产对比报表模板			v
*报表文件格式:	注:系統模版默认只生成漏洞权重 💟 Word 版 💟 HTML 版 🗌	大于 50% 的漏洞,如需更改请使用自定义模版 PDF 版		管理报表模板
* 统计时间单位:	〇天 🧿 WEEK 🔘 MONTH	SEASON		
	选择目标主机			清空已选目标
	资产地址	所属组织单位	标签	操作
	10.3.2.134	默认工作区		mist
	10.3.2.142	默认工作区	-	删除
	10.3.2.114	默认工作区		副除
				< 1 > 取消 确定

删除主机:

在主机资产列表页可以主机资产进行批量删除,一旦执行了删除操作,所有选中的 主机资产信息均将被删除,具体操作为:

- 选中要删除的主机资产,此时显示已选择的主机资产总数;
- 点击"删除选中的主机"按钮,提示框提示确定是否删除,点击"确定",则删 除成功。



⑦ 全局仪表盘		(remain	明单位	默认工作区 X (存活性 存活 X)	+ 液加筛透条件	Ŧ									\$
□ 扫描管理	×.	• e	选择 2	个主机					存活动	哧 …	T	社業損作 🗸	+ #	ন্টার্টা	e主机
6 基线管理	٧			资产地址	内部负责人	所属组织单位	业务系统	风险等级	NAB	ante.		日は まつ	操作		
き 西戸中心	^		•	10.3.0,112	admin	默认工作区		无风限		10	8	编辑	28	10.91	80
前产利表				10.3.0.8	admin	赋认工作区		满风微	٥		E.	与此 生成报表	26	1618	-
主机银产列表	1		•	10.3.0.111	admin	默认工作区	100	无风险			1	下发任务	26	ME ST	-
Web 站点资产	列表		•	10.3.0.7	admin	默认工作区	553	无风险	13	8	8	8	26	5518	8638
资产相列表			•	10.9.33.32	admin	默认工作区		美风胜	13	ш			20	1818	-
资产属性管理	*		•	10.3.0.8	hyl03	默认工作区-hyl01-hyl02		王风殿					26	5651	19130
△ 派羽管理			•	10.3.0.6	hyl03	默认工作区-hyl01-hyl02	1370	高风暗	- 13		0		26	1818	86.38
a 报表中心	Υ.			10.3.0.210	hyl01	默认工作区-hylD1	323	无风险	13			123		1610	-
圆 知识库	*			10.9.33.70	admin	默认工作区		王风龄		13				1618	-

编辑选中的主机:

- 选中要编辑的主机资产,填写目标信息
- 点击确定或者取消操作

默认工作区	\vee	前产中心 /	30.03	1長 / 主机资产列表											
◎ 全局仪表盘		TEM	包织单位	默认工作区 × 7 存活性 存得	舌 ×) + 液加筛透条	件									٢
日 田橋管理	×	• E	选择。	2 个主机					存活动	応 …	E	出版作。>	+ #	លគេស	主机
必 基线管理	*			资产地址	内部负责人	所屬組织单位	业务系统	风险等级	漏洞数	*		128	操作		
意 商产中心	~										3	前空 448			
资产全景			•	10.3.0.112	admin	默认工作区		王凤鹿	- 10	. 63		9出	28	10.11	新祥
RPHR.				10.3.0.8	admin	赋认工作区		萬风險	3		E g	E成报表	26	1810	-
主机语产列表		I II	•	10.3.0.111	admin	赋认工作区		无风险				下发任务	26	1011	H 70
Web 站点资产	•列表	12	•	10.3.0.7	admin	默认工作区	1.50	无风险	13	0	8	8	26	55.12	8038
资产组列表				10.9.33.32	admin	赋认工作区		死风险	13	Ш.			24	1838	-
资产属性管理	*		•	10.3.0.8	hyl03	默认工作区-hyl01-hyl02		无风险	13		8		28	5610	#63R
△ 漏洞管理				10.3.0.6	hyl03	默认工作区-hyl01-hyl02	1.52	高风間	- 10		8		26	-	8638
□ 报表中心	¥.			10.3.0.210	hyl01	默认工作区-hyl01	120	无风险	0			0		16.10	B 12
0 mar	*			10.9.33.70	admin	默认工作区	-	王风的						1618	111 A

资产地址	10.2.19.111 192.168.181.100	
资产名称	3-28-67-62393	
所在地址	为改革用于研究原植	
组织单位		
负责人		
资产权重	为党政师书研究团组	
业务系统	为空表示不够改原情	
网络区域	3-28-7-928-8	
标准	1012/01/07	



快速扫描主机。

在主机资产列表页可以对选中主机资产进行快速扫描,具体操作为:

- 选中要扫描的主机资产,此时显示已选择的主机资产总数;
- 当以选中主机资产创建扫描任务时,创建的扫描任务名称会自动变为:"任务名称+所在组织单位名称"
- 点击"批量操作"-"下发任务"按钮,跳转至添加扫描任务界面添加扫描任务界面,扫描目标处会自动填写进第一步中选中的主机资产,具体参数 配置参考 3.1.5 添加扫描任务。



全局仪表盘		(remain	明单位	默认工作区 X (存活性 存活 X)	+ 滚加筛透条	件									W.
目描葉理	×	0 B	选择 2	个主机					存活动	応 …	M	社業調作 マ	+ #	আরি	e主机
《基线管理	*			资产地址	内部负责人	所觸組织单位	业务系统	风险等级	漏洞器			BIR	操作	č.	
* 资产中心	^	-		1030112	admin	制动工作的						加至	-	10.40	auto.
资产全景		-	0.	Constant for	and the second s	an weater as					1	导出	-		-
nr Ha				10.3.0.8	admin	赋认工作区		高风微	3		1	生成报表	26	1918	B(B)
主机资产列表			•	10.3.0.111	admin	默认工作区	100	无风险	0	0		下发任务		14110	H 20
Web 站点资产	列表		•	10.3.0.7	admin	默认工作区		无风险	13	0	13	1 11		5511	B (34
资产组列表			•	10.9.33.32	admin	默认工作区		光风险	13	Ш.	8	I II	26	1818	B 10
资产属性管理	*		•	10.3.0.8	hy103	默认工作区-hyl01-hyl02		无风险			8		28	1610	11(32
漏洞管理				10.3.0.6	hyl03	默认工作区-hyl01-hyl02	353	高风暗	13		0			1818	853
报表中心	Υ.			10.3.0.210	hyl01	默认工作区-hylD1	122	无风险	13			1 (2)	-	1610	2 (1)
如识库	~			10 9 33 70	admin	瞬日本街屋	-	2.04	-	-				40.40	

<·>洞鑒 _{x-n}	IAY	
默认工作区	V BE	NIT / EXPLANT WANTERER
◎ 全局仪表盘		任务基本信息
15 扫描描述	w	扫描 常端 希望 新拉拉外面同行派
8 基线管理	*	· · · · · · · · · · · · · · · · · · ·
8 8/540		2.218 MOTION 1
前广王甫		扫描描篇自动同步 🛇
百产和表	*	*任务表展 潮汕
主机而产列表 Web 站在用户》	10	83
后产组织表		
百广英档管理	* [定时扫描
- MULT		18.000 4004
1 相表中心		WITHE ASSESS
□ \$290(JE	*	銀電射視機 ③ 🙃 指定于目的1段 —— 指定 M E351段
- **I##	Č	高加州百姓 明明
- H2"ER	·	
		扫描目标
		- 4504 BULDE

< → 洞鉴 x-	RAY									ad	imin
默认工作区	~	onen i	任务列表								
◎ 全地位表盘		(MINUS	50年位 默认工作区 X	十 透加薄选条件							
日白檀香酒	. e.:	0 E	选择 0 个扫描任务						批單操作 >	+ 1640131813	£15
A 基础管理	- 943		扫描任务名称	风险等级	扫描策略	创建用户	所属组织单位	扫描状态	最近扫描时间	議作	
き 資产中心		-									
资产主席		L	测试-默认工作区	34 	基础服务漏洞扫描	admin	默认工作区		*	D	
治产利表			detest	8.8.10	基础 Web 漏洞扫描	admin	默认工作区	③ 扫描结束 (成功)	2023-04-19 19:01:22		
主机资产利用			detail-test	RAR	基础 Web 漏洞扫描	admin	默认工作区	④ 扫描结束 (手动结束)	2023-04-19 18:59:42	D	
Web 贴点资产	*判核										
治产组列表			asdiasdfasd		基础服务漏洞扫描	admin	默认工作区	*	*		
资产属性管理			12345		基础服务漏洞扫描	admin	默认工作区				
· 運用管理	्		1	4.000	基础服务漏洞扫描	admin	默认工作区	 () 扫描结束 (手动结束) 	2023-04-19 14:44:10		
回 経費中心											
CI 1064			日志	9.830	基础服务漏洞扫描	admin	默认工作区	② 扫描结束 (成功)	2023-04-14 14:46:10		
◎ 苏杭繁理	120		自名单问段 存在问	无风险	基础服务漏洞扫描	admin	默认工作区	② 扫描结束 (手动结束)	2023-04-19 14:39:50		
A 用户管理	1		test	2.5.M	基础 Web 漏洞扫描	admin	默认工作区	③ 扫描结束 (成功)	2023-04-18 19:34:32	Þ	



导出选中的主机:

在主机资产列表页可以选择多个主机并导出所选主机的地址,具体操作为:

- 选中希望导出的主机地址,此时显示已选择的主机资产总数,同时"导出"按钮变为可点击状态;
- 点击"导出",系统将自动把选中的资产地址存为 txt 文件。

默认工作区	\vee	第产中心 /	375	「長 / 主机资产列表											
○ 全局仪表盘		Стеща	包织单位	默认工作区 × 7 存落性 存	活 × + 液加筛选条	件									\$
⊖ 扫描管理	×	• E	选择:	2 个主机					存活动	応 …	ſ	社能操作 >	+ #	ain t	e主机
杀 基线管理	¥			资产地址	内部负责人	所属组织单位	业务系统	风险等级	派河势	*		eite	操作		
意 商产中心											H	清空			
资产全额			•	10.3.0,112	admin	默认工作区		王凤窟	- 13	10	4	编辑	28	18.98	80
8×10				10.3.0.8	admin	赋认工作区		满风散	3	0	1	生成报表	26	1818	-
主机资产列表		Π	•	10.3.0.111	admin	赋认工作区		无风险	-			下发任务	26	1018	-
Web 站点资/	**判表		•	10.3.0.7	admin	默认工作区		无风险	13	0	12	8		55.12	8138
资产组列表			•	10.9.33.32	admin	赋认工作区		光风险	13	Ш.			26	1818	-
资产属性管理	*		•	10.3.0.8	hyl03	默认工作区-hyl01-hyl02		无风险	0	13			28	5611	R (38
△ 漏洞管理				10.3.0.6	hyl03	默认工作区-hyl01-hyl02	1.52	高风暗	10		0		-	-	81.38
□ 报表中心	×			10.3.0.210	hyl01	默认工作区-hyl01		无风险	13					1610	-
囗 批词库	*			10.9.33.70	admin	默认工作区	(140)	王凤龄	0					1611	100 A
A Research															

存活动态快速筛选:

在主机资产列表页可以配置时间维度和动态维度,来查看一段时间内资产存活性的 动态变化:

		三 / 主机资产列表								
CAR		RAIME X) (nam	配置箨选条件		×					0
0 8	28.FF (个主机	时间范围 🥑 本天 🔘 本	周 🔾 本月		413	Ritifi	-	社業純作 ッ	+ 平和高加主机
		资产地址	动态设置 💽 新場存活 🗌	新增失活 🔘 波动变化	_	R [12]	x AM			18:17
	•	10.9.33.70			取別 保存					
		10.9.33.148	admin	默认工作区	MRM	۰				
		10.8.33.32	admin	默以工作区	RRA					
	-	10.3.0.4	admin	默认工作区	RBM					
		10.3.0.7	admin	献从工作区	无用能					
	•	10.3.0.1	admin	默认工作区	(ANN)					
		10.3.0.8	admin	默以工作区	(ARM)					
	-	10.3.0.5	admin.	默认工作区	无风度					
		10.3.0.6	admin	默认工作区	(未5前)					
		10.3.0.209	admin	默认工作区						



对于筛选后的资产,可以在资产地址后面看到"新增存活"、"新增失活"、"波动次数"的标签,点击标签,可以查看资产存活性变化的情况。





3.4.2.2 主机资产详情

在主机列表处, 点击"查看", 即可打开主机详情界面。

内容展示:

主机详情页顶部主要展示主机的资产名称,组织单位,创建时间,业务系统,所在 地址,标签,网络区域,负责人及资产风险等级图标:

 西产名称 - 业务系统 - 资产权重 3 	維約単位 所在地址 网络区域	默认工作区 中国/北京7 -	1 5/东城区		倒錄时间 标签 负责人	2021-12-02 14:35 - admin	:59	高风险		13 Materia	185
第口指纹信息 主机漏洞信息	Web 信息										
纹情况		建口情况 含素	民间撤给果伙计	ø							15.tote
运营商 IP		端口	协议	服务	ŕ	5	版本	操作		1	
位置 局域网		5357	TCP	top	8			1618	#178		
F系统 Windows 🧷		49156	TOP	top	2			LE TR	图珍	•	
12 - 2		1025	TCP	top	×			197.50	删除		
o nation -		49152	TCP	msrpc	Mi	crosoft Windows R		1010	副時		
		49153	TCP	msrpc	Mi	crosoft Windows R		Se car	删除		
		49154	TCP	marpc	M	crosoft Windows R		編輯	删除		
		49155	TCP	merpo	м	crosoft Windows R		编辑	#113	•	

端口指纹信息:

此选项主要展示当前主机资产的指纹情况与端口开发情况,包括 IP 运营商, IP 位置, 设备类型,操作系统,主机名,端口,协议,服务,产品,产品的版本(如上图所示):

- 设备类型可以在此手动修改,点击设备类型右侧的图标即可编辑;
- 操作系统可以在此手动修改,点击网络区域右侧的图标即可编辑;
- 主机名可以在此手动修改,点击主机名右侧的图标即可编辑。

主机漏洞信息:

此选项卡主要展示与当前主机相关的所有漏洞信息,内容包括漏洞名称、漏洞等级、 漏洞权重、存在漏洞的位置、发现时间:



將列表 历史变化						
添加筛选条件						
第 羽名称	漏洞等级 ;	漏洞权重	濕潤編号	漏洞位置	温润状态	发现时间 😄
WE-2020-14859: Oracle WebLogic Server Core 史	-	99%	CT-144010 CVE	10.3.0.202:7001/TCP	● 待分配 ∨	2021-12-16 10:52:13
VE-2020-2551: Oracle Fusion Middlewara WebLo	-	99%	CT-26370 CVE	10.3.0.202:7001/TCP	• 待分配 ~	2021-12-16 10:52:13
/E-2020-2555: Oracle Utilities Framework 安全運調	#.N.	99%	GT-64462 CVE	10.3.0.202:7001/TCP	• 待分配 >>	2021-12-16 10:52:13
/E-2020-14687: Oracle Fusion Middleware WebL	-	99%	GT-44679 CVE	10.3.0.202:7001/TCP	• 待分配 ~	2021-12-16 10:52:13
rE-2020-2915: Oracle Fusion Middleware 安全運調		99%	CT-129019 CVE	10.3.0.202:7001/TCP	• 待分配 ~	2021-12-16 10:52:13
E-2020-14841: Oracle WebLogic Server Core R	-	99%	CT-144454 CVE	10.3.0.202:7001/TCP	● 待分配 >>	2021-12-16 10:52:13
OVE-2020-14645: Oracle Fusion Middleware Webl		00%	CT-123539 CVE	10.3.0.202:7001/TCP	• 简分配 V	2021-12-16 10:5

- 点击"风险等级"、"发现时间"右侧的三角图标,可以将列表按风险等级、发现时间升序或者降序排列;
- 点击漏洞名称,可以跳转至漏洞详情页面。

Web 信息:

此选项卡主要展示与当前主机相关 web 站点信息,内容包括 web 站点地址:

指纹信息	主机漏洞信息	Web 低思
http://10.3.0.202:70	01/	
http://10.3.0.202/		



3.4.3 Web 站点资产列表

在左侧导航栏中,选择"资产中心-资产列表-Web 站点资产列表",进入 Web 站 点资产界面。

<->洞甇x-RA	ĸ											admin
默认工作区	/ 1	12年67月	百广刊卷 / Web 站点资产列表									
◎ 全局仪表盘		Cressel	5.000 默认工作区 ×) + 添加?	8送条件								0
8 日間管理	÷	• Ež	5择 0 个 Web 站点							批集	1線作 〜	十 手动道加鼓点
A 圣线管理	¥ .		资产地址	内部负责人	所属组织单位	业务系统	风险等级	漏洞委	ŧ#			操作
◎ 资产中心	^]		http://10.3.0.8:49153/	admin	默认工作区		15,7,10	13	13	0	8	
资产全 费			https://10.3.0.6:8443/	admin	默认工作区	2	ISAN .		13		-	-
主机资产列表			http://10.3.0.8:49155/	admin	默认工作区	×	(EAN)		0		0	
Web 站点语产列表			http://10.3.0.8:49156/	admin	默认工作区		(BAR)		13	0	67	28 mil 970
图户:组列表	J		http://10.3.0.8:8888/	admin	默认工作区	-	(15.R.B)	0	13		0	
资产属性管理	*		http://10.3.0.6:8080/	admin	默认工作区		任风险	0	13	0	8	重要 编辑 删除
△ 漏洞管理	e:											10 卷/西 🗸
> 服務中心	¥.											
□ 知识库	÷				X-Ray XR-50-0 10-2	3.02.001_121 @ 2022 Challin	Tech.					



3.4.3.1 Web 站点资产列表

内容展示:

主要展示所有的 Web 资产信息,内容包括资产地址、负责人、所属组织单位、业务系统、风险等级和各等级下漏洞数量:

E	选择 0 个 Web 站点							3	t量操作 ~	+ 手	动激动	in Na
	资产地址	内部负责人	所属组织单位	业务系统	风险等级	漏洞數				操作		
ł.	http://10.3.0.8:49153/	admin	默认工作区	-	低风险	.0	8	۵	0	童術	编辑	191
	https://10.3.0.6:8443/	admin	默认工作区	120	低风险	10			0		su	m
	http://10.3.0.8:49155/	admin	默认工作区	107-1	(ILMIN)			8	6	88	编辑	-
	http://10.3.0.8:49156/	admin	默认工作区	181	低风险				0	26	55 ¥I	10
	http://10.3.0.8:8888/	admin	默认工作区	(*)	低风险	8	63		6	查看	编辑	-
	http://10.3.0.6:8080/	admin	默认工作区	1.2	低风险		10			-	1618	

筛选 Web 站点:

在 Web 资产列表页可对 Web 站点资产进行筛选操作,可根据资产地址、风险等级、负责人、组织单位、业务系统、标签、网络区域、资产名称、所在地址、web 应用、 网站 title、开发语言、CMS、WAF、CDN,自由添加一个或多个条件进行筛选,具体 操作为:

- 点击"添加筛选条件"按钮,弹出添加筛选条件对话框;
- 选择要增加的筛选条件类型并填写相应的要筛选的内容;
- 点击"增加一个筛选条件",可以增加筛选限制条件;
- 点击"删除",可以删除掉不需要的筛选限制条件;
- 筛选条件限制至少要添加一条;
- 设置好条件后,点击"保存",即可展示符合筛选条件的列表。



添加筛选条件			>
资产地址	~	请输入要筛选的内容	模糊匹配∨
+ 添加筛选条	件		
			取消保存

添加 Web 站点:

在资产列表页可以通过手动添加一个或导入 cvs 文件的方式添加资产, 方便管理员添加企业资产, 具体操作为:

- 在列表页点击"+ 手动添加 XX 资产",显示填写内容的弹窗
- 选择添加方式:
 - 添加一个资产
 - 上传资产文件
- 按照不同方式的添加要求,填写资产相关信息;
- 点击"确定"按钮,完成资产添加。
- 注意:
 - 已经存在的资产不能被重复添加;
 - 上传文件格式必须严格按照模板提供的格式添加,不同资产列表的模板不一
 样,请下载查看。

动激加贴点		
学动植物	文件上传	
* 资产地社	信頼入多でVino 2011、多で信户発行対策、共初 1992/11.2.3.4.4050 1999x/11.2.3.4.9503 3359//Www.shatiin.ch/	
		h
资产名称	请输入资产名称对资产进行错误	
*所在地址	北京市/东城区	
* 暗积单位	氟化工业资	
*负责人	admin	
资产组	建造得资产组	
* 资产权重	3	
业务系统	诸遗理资产历期业务系统	
网络区域	法法律资产所属网络区域	
标签	+ 18.10	



生成 Web 站点资产报表:

在 Web 站点列表页可以选择多个 Web 站点并生成所选站点的报表(如下图所示),具体操作为:

- 选中希望生成报表的 Web 站点资产,此时显示已选择的 Web 站点资产总数,同
 时"批量操作"-"生成报表"按钮变为可点击状态;
- 点击"批量操作"-"生成报表"按钮;
- 在弹出的窗口中,选择相应的生成配置;
- 点击"确认",即可开始生成报表。可以前往报表管理页面查看报表生成的情况, 或下载生成好的报表。

Ei	选择 2 个 Web 站点								批量操作 ~	+ 準	动廠	加站点
	资产地址	内部负责人	所属组织单位	业务系统	风险等级	漏洞對	量		删除 清空	操作		
1	http://10.3.0.8:49153/	admin	默认工作区	21	低风险				编辑	29	1918	剧林
J.	https://10.3.0.6:8443/	admin	默认工作区	-	低风险			L	下发任务	皇君	UQ 10	H13
	http://10.3.0.8:49155/	admin	默认工作区	-	低风险		8	63		没有	till Fill	211 3
	http://10.3.0.8;49156/	admin	默认工作区	~	任风险			0		宣有	iste	B 13
	http://10.3.0.8:8888/	admin	默认工作区	-	任风险			13		度看	编辑	影除
	http://10.3.0.6:8080/	admin	默认工作区	2	低风险			0	3	波看	編輯	EIR


*报表名称:	https://10.2.19.111/的资产报表			
* 所屬组织单位:	WUITE			
*报表类型:	而产指表			
*报表模板:	; 资产报表模板			
* 报表文件格式:	Nord版 💟 Excel版 💟 HTML版 🗌 PDF版			
* 报表目标:	 ● 主机和 Web 站点 ● 资产组 透择目标主机 			清空已送目标
	资产地址	所属组织单位	标签	操作
		新天教編		
	选择目标 Web 站点			清空已选目标

编辑选中的 Web 站点:

- 选中要编辑的主机资产,填写目标信息;
- 点击确定或者取消操作。

E	告择 2 个 Web 站点								批量操作 ~	- + 準	动流	加站点
1×	资产地址	内部负责人	所翼组织单位	业务系统	风险等级	漏洞數	遭		删除 清空	操作		
2	http://10.3.0.8:49153/	admin	默认工作区	1	低风险				编辑	20	1918	R IB
2	https://10.3.0.6:8443/	admin	默认工作区	-	低风险				主成报表 下发任务	28	10,11	#13
	http://10.3.0.8:49155/	admin	默认工作区	0	低风险			13		没有	编辑	B128
	http://10.3.0.8;49156/	admin	默认工作区	-	低风险		13		67	查看	ista	B [13
	http://10.3.0.8:8888/	admin	默认工作区		任风险					度看	编辑	删除
	http://10.3.0.6:8080/	admin	默认工作区	2	低风险		10	0	3	波看	1918	B(1 8

删除选中 Web 站点:

在 Web 站点列表页可以对 Web 站点资产进行批量删除,一旦执行了删除操作, 所有选中的 Web 站点资产信息均将被删除,具体操作为:



- 选中要删除的 Web 站点资产,此时显示已选择的 Web 站点资产总数,同时"删
 除选中的 Web 站点"按钮变为可点击状态;
- 点击"删除选中的 Web 站点"按钮,在弹出的是否确定删除的提示框中,点击"确定",则删除成功。

Ei	选择 2 个 Web 站点								批量操作 ~	- + 準	动滚	10185)
i e	资产地址	内部负责人	所属组织单位	业务系统	风险等级	漏洞對	۲ <u>۳</u>		删除 清空	操作		
2	http://10.3.0.8:49153/	admin	默认工作区	÷.	低风险				编辑	29	1918	B()
	https://10.3.0.6:8443/	admin	默认工作区	-	低风险			L	下发任务	皇君	UR FR	-
	http://10.3.0.8:49155/	admin	默认工作区	-	低风险	13	8	53		没有	til Hi	-
	http://10.3.0.8:49156/	admin	默认工作区	~	低风险			0	0	宣有	iste	-
	http://10.3.0.8:8888/	admin	默认工作区	-	任风险				•	度看	编辑	- MI
	http://10.3.0.6:8080/	admin	默认工作区	2	低风险		10	0	3	波看	编辑	-

快速扫描 Web 站点

在 Web 站点列表页可以对选中 Web 站点资产进行快速扫描,具体操作为:

- 选中要扫描的 Web 站点资产,此时显示已选择的 Web 站点资产总数,同时"批 量操作"-"下发任务"按钮变为可点击状态;
- 点击"批量操作"-"下发任务"按钮,跳转至添加扫描任务界面;
- 添加扫描任务界面,扫描目标处会自动填写进第一步中选中的 Web 站点资产
- 当以选中 Web 站点资产创建扫描任务时,创建的扫描任务名称会自动变为:"任务
 名称+所在组织单位名称",同主机资产。
- 在添加扫描任务界面,具体参数配置参考<u>3.1.5添加扫描任务</u>。



0 E	选择 2 个 Web 站点								批量操作 ~	+ 準	动液	加站
• •	资产地址	内部负责人	所属组织单位	业务系统	风险等级	漏洞數	大量		删除 清空	操作		
	http://10.3.0.8:49153/	admin	默认工作区	20	低风险				编辑	29	1918	開胡
~	https://10.3.0.6:8443/	admin	默认工作区		低风险	0			下发任务	28	10110	B (1)
	http://10.3.0.8:49155/	admin	赋认工作区	a	低风险			(1)	•	宣看	1010	B(1)
	http://10.3.0.8:49156/	admin	默认工作区	5	低风险		13	13	07	查看	ista	B IN
	http://10.3.0.8:8888/	admin	默认工作区	-	任风险			13	•	度看	编辑	影除
	http://10.3.0.6:8080/	admin	默认工作区	2	低风险		12	0	3	沒有	1818	BIN



3.4.3.2 Web 站点资产详情

在 Web 站点资产列表处, 点击"查看", 即可打开 Web 站点详情界面。

内容展示:

此页面顶部展示 web 资产的资产名称,组织单位,创建时间,业务系统,所在地址,标签,资产权重,网络区域,负责人,资产风险等级图标以及待处理风险数:

					-	
资产者称	· 组织(位 默认工作区	包螺时间	2021-12-14 17:11:22		
业务系统	- 所在:	地 中国/北京市/东城区	杨雅	32		22
资产权置	3 网络日	3堆 -	负责人	admin	高风险	PERCENT PLANERS
Web 指纹信息	Web 漏洞信息 目录结构信息	子域名信息 主机信息				
-						
http://s2-046.vul.c	±8191/					
http://s2-046.vul.c 指纹情况	L8191/	Web 情况				湖山 Web 近刑
http://s2-046.vul.c 指纹情况 网站 Title	E8191/ Error 404 /external/pages/upload-success.jsp	Web 情况 Web 应用	应用	問題本	8	浅油 Web 应用
http://s2-046.vul.c 指纹情况 网站 Title 开发语言	E8191/ Error 404 /external/pages/upload-success.jsp	Web 開況 Web 庭用	应用	超本	8	路加 Web 应用 作
http://s2-046.vul.c 脂纹情况 网站 Title 开发语言 CDN 鲜析	E8191/ Error 404 /external/pages/upload-success.jsp -	Web 情况 Web <u>后</u> 用	应用	8基本	8	简加 Web 应用 作
http://s2-046.vul.c 脂纹情况 网站 Title 开发语言 CDN 歸所 WAF 识别	E8191/ Error 404 /external/pages/upload-success.jsp - -	Web 维况 Web 应用	应用	164×		后加 Web 应用

Web 指纹信息:

此选项卡内主要展示 Web 资产的指纹情况与 Web 情况,包括网站标题,开发语言, CDN 解析,WAF 识别,CMS 识别,原始 banner 及 Web 应用与应用版本,支持对应 用及应用版本进行添加、编辑与删除(如上图所示):

- 点击查看原始 banner 可查看原始 banner;
- 点击"添加 Web 应用"可以手动添加 web 应用,点击"编辑"可以编辑 web 应用 名称与版本号,点击"删除"可以删除 web 应用。

Web 漏洞信息:

此选项卡内主要展示当前 web 资产的漏洞信息,包括漏洞名称,漏洞等级,漏洞 权重,漏洞位置,发现时间。



- 点击"风险等级"、"发现时间"右侧的三角图标,可以将列表按风险等级、发现
 时间升序或者降序排列
- 点击漏洞名称,可以跳转至漏洞详情页面

Web 獨纹信息 Web 瀰濁信息 目录结	纳信息 子城	名信息 主机	信息			
 講習所表 历史变化 + 添加等送条件 						
漏洞名称	漏洞等级 ;	漏洞权重	漏洞编号	漏洞位置	還洞状态	发现时间 😄
CVE-2017-5638: Apache Struts 2 输入验证错误漏洞	E	99%	CT-30789 CVE	http://s2-046.vul.ot:8191/doUpload.a	● 待分配 ∨	2021-12-14 17:45:11
CVE-2017-5638: Apache Struts 2 输入验证错误编制	-	99%	CT-30789 CVE	http://s2-048.vul.ct:8191/external/	● 特分配 >	2021-12-14 17:45:06
CVE-2017-5638: Apache Struts 2 输入验证错误漏洞	FB	99%	CT-30789 CVE	http://s2-048.vul.ct:8191/config/	• 待分配 ~	2021-12-14 17:44:58
CVE-2017-5638: Apache Struts 2 输入验证错误展测	78	99%	CT-30789 CVE	http://s2-046.vul.ct:8191/	• 待分配 ~	2021-12-14 17:44:57
HTTP 朝应头 Server 建晶榄菜信息漏洞	E .R	99%	*	http://s2-048.vul.ct:8191/external/	● 待分記 ∨	2021-12-21 16:09:44
HTTP 前应头 X-Frame-Options 缺失(点击结持)	65.8	99%		http://s2-046.vul.ct:8191/external/	• 待分配 ~	2021-12-21 16:09:44
HTTP 第应头 X-Content-Type-Options 缺失漏洞	(6.8)	99%	8	http://s2-046.vul.ct:8191/external/	• 待分配 >>	2021-12-21 16:08:44

目录结构信息:

此选项卡以结构树形式展示了 web 站点的结构:

● 点击目录左侧的图标可以展开或收起。

http://c2-046.vul.et/8191/ config/ doUpload.action	Web 指纹信息	Web 漏消信息	日录结构信息	子域名信息	主机信息			
config/ doUplead.action	+ http://s2-046.vt	ul.ct:8191/						
doUpload.action	config/							
	doUpload.actio	n						

子域名信息:

此选项卡以结构树的形式展示了该 Web 资产下的子域名:

● 点击目录左侧图标可以展开或收起

主机信息



此选项卡展示了与该 web 资产相关的主机 ip:

Web 指纹信息	Web 漏詞信息	目录结构信息	子城名信息	主机信息
解析 IP: 10.3.0.5				



3.4.4 资产组列表

在左侧导航栏中,选择"资产中心-资产列表-Web站点资产列表",进入资产组界面。

								admin
默认工作区	~	目の中心 / 国内列表 / 資产組列表						
② 全局仪表盘		(新鳳組织単位 默认工作区 ×) + 3	泰加等选条件					
日 扫描管理	~	 已选择 0 个资产组 					○ 批量操作 >	+ 添加资产组
<i>A</i> 基线管理		资产组名称	备注	所属组织单位	负责人	标签	资产同步模式	创建时间
意 资产中心	~	测试资产组		财认工作区	admin		手动同步	2024-02-26 17:4/
资产全景	- 1			APT O'COLLT NAME			3 40 35	
资产列表	~						共1条 < 1	> 10 条/页 ~
主机资产利	A			v n., vn esa		NAME OF THE OWNER.		
Web 站点窗	产列表			Arriay Arriang	10-24.02.001.34 9	2024 Unitarin Jeon.		
资产组列表								
资产属性管理	*							
合 運動管理	~							
自 报表中心	*							
囗 知识库	×							
② 系统管理	×							
△ 用户管理								



3.4.4.1 资产组列表

内容展示:

主要展示所有的资产组信息,内容包括资产组名称、备注、所属组织单位:

● 已选择 0 个资产组					0	批量操作 ~	+ 添加资产组
资产组名称	备注	所属组织单位	负责人	标签		资产同步模式	创建时间
测试资产组		默认工作区	admin	2		手动同步	2024-02-26 17:4

添加筛选条件:

同 3.4.2.1 主机资产列表。

生成报表:

同 3.4.2.1 主机资产列表。

删除选中的资产组:

同 3.4.2.1 主机资产列表。

快速扫描资产组

同 3.4.2.1 主机资产列表



3.4.4.2 添加资产组

在资产组列表处, 点击"·	- 添加资产组"	即可打开添加资产组界面	(如下图所示):

		admin
默认工作区	✓ 首作中心 / 首作利用 / 首作相列表 / 添加資产者	
◎ 全雨仪表盘	* 资产组名	3 简能入现产组合和
日 白服物理		
A 基线管理	× 6	₫ 間個人音注
意 资产中心	∽ *所属组织单	2 默认工作团 🗸
资产全景	* 负责	K admin
资产列表	*	
主机资产列	联系劇	A Transmitta (F) (ART) (ART) (ART) (ART) A A A A A A A A A A A A A A A A A
Web 站点资	产列表	
资产组列表		
资产属性管理	×	任务发送报表通知 ⑦ 🔘
☆ 混彩管理	~ 桁	至 十 滅加
直 报表中心	* 资产同步模式	9 ● 手动同步
圓 她说库	~	
② 系统管理	↓ 目标主机图	"IP地址 操作系统 所属组织单位 备注 操作 从宽广列表导入
△ 用户管理	× .	

具体操作如下:

- 输入资产组名称,不能为空;
- 选择性输入备注内容;
- 选择所属组织单位
- 选择负责人
- 联系邮箱
 - 一个资产组可绑定多个联系邮箱,当开启"任务发送报表通知"按钮时,针对该资产组下发的任务所生成的扫描报表(只针对开启"自动生成扫描报表"的任务) 会发送至该资产组绑定的联系邮箱。
- 标签
- 选择资产同步模式
 - 手动同步:
 - ◆ 点击 "从资产列表导入", 弹出弹窗, 选择要添加的主机资产 (如下图所示):



选择需要导入的	主机资产				×
资产地址:		标签:		存储性: 存活 ×	
	资产地址		所属组织单位	标签	
	10.9.33.70		WUINE		
	10.9.33.148		NULTE	(5)	
	10.9.33.32		默认工作区		
	10.3.0.4		默认工作区		
	10.3.0.7		服以工作区		
	10.3.0.1		取以工作区	2	
	10.3.0.8		服以工作区	2	
	10.3.0.5		服以工作区	2	
	10.3.0.6		服以工作区	(5)	
	10.3.0.209		服认工作区	5 C	
				< 1 2 3 > 10条/页〜 職室	π
					-

◆ 点击"选择目标 Web 站点",弹出弹窗,选择要添加的 Web 站点资产。

选择需要导入的	Web 站点资产				
资产地址:		杨雅:			
	西产和社		所属组织单位	相查	
	https://10.3.0.4:8443/		服以工作区-byi01-by/02-byi03	2.	
	https://10.3.0.4/		服认工作语-hyl01-hyl02-hyl03		
	http://10.3.0.4/9000/		图以工作区-hyl01-hyl02-hyl03		
	http://10.3.0.4;3000/		默认工作经-hyl01-hyl02-hyl03		
	https://10.3.0.4;8080/		副U.I.作匠-ty/01-ty/02-ty/03		
	http://10.3.0.4;8061/		間以工作区.hyl01-hyl02-hyl03		
	http://10.3.0.4:5000/		服以工作区-hyl01-hyl02-hyl03		
	http://10.3.0.4.8888/		IIIS认工作区-hyl01-hyl02-hyl03		
	http://10.3.0.8:49153/		服以工作区-3y/01-3y/02		
	http://10.3.0.8:49167/		1051、工作这一by/01-hy/02		
			< 1 2 3 4	5 28 > 10条/页- 建亚	
				2.2	-

- ◆ 点击"完成"成功添加新资产组。
- 自动同步:
 - ◆ 当前可以以 IP 段为维度, 配置自动同步的字段

* 资产组名称	请输入资产组名称	
	资产组名称不能为空	
备注	请输入者注	
* 所属组织单位	默认工作区	
资产同步模式 ②	○手动同步	
* IP 段 ③		
	P段不能为空	



◆ 点击"完成"成功添加新资产组。

3.4.4.3 手动类型资产组列表编辑

在资产组列表处,点击手动同步类型资产组的"编辑",即可打开编辑资产组界面(如下入所示):

* 资产组名称	一个资产组								
备注	谱输入描注								
* 所属组织单位	默认工作区								
8产同步模式 ⑦	手动同步								
目标主机资产	IP 地址	操作	系统	所罵组织单位	ġ.	备注		操作	从资产列表导入
	10.9.33.70	Ubu	ntu	默认工作区				删除	
	10.3.0.8	Wine	iows	默认工作区-	hyi01			删除	
	10.3.0.5	Ubu	ntu20.04	默认工作区-	hyl01			MIR	
							< 1 >	10 条/页 ∨	
目标 Web 资产	资产地址	Web 站点标题	所属组织	识单位	备注			操作	选择目标 Web 站点
				暫无数提	1				

具体操作如下:

- 可修改资产组名称,不能为空;
- 可修改备注内容;
- 所属组织单位和资产同步模式不可更改;
- 点击"从资产列表导入",弹出弹窗,选择要添加的主机资产:

选择需要导入的	主机资产				>
8产地址:		标签:		存活性: 存语 ×	
	夏产地址		所覆组织单位	标准	
	10.9.33.70		献以工作区	÷.	
	10.9.33.148		服以工作区	5	
	10.9.33.32		默认工作区	19 A	
	10.3.0.4		服认工作区		
	10.3.0.7		服认工作区		
	10.3.0.1		跟以工作区	2	
	10.3.0.8		默认工作区	2	
	10.3.0.5		联队工作区	2	
	10.3.0.6		服以工作区		
	10.3.0.209		默认工作区		
				< 1 2 3 > 10 条/页 · 藏至	1
				10.10	前定



● 点击"选择目标 Web 站点",弹出弹窗,选择要添加的 Web 站点资产:

选择需要导入的	Web 站点资产			
资产地址:		15首:		
	西产和社		所属组织单位	标签
	https://10.3.0.4:8443/		服认工作区-hyl01-hyl02-hyl03	
	https://10.3.0.4/		服认工作语-hyl01-hyl02-hyl03	4)
	http://10.3.0.4/9000/		置以工作包-hyl01-hyl02-hyl03	
	http://10.3.0.4:3000/		默认工作这-hyl01-hyl02-hyl03	
	http://10.3.0.4;8080/		副以工作区-hyl01-hyl02-hyl03	
	http://10.3.0.4;8081/		服以工作区-hyl01-hyl02-hyl03	
	http://10.3.0.4:5000/		默认工作这-hyl01-hyl02-hyl03	
	http://10.3.0.4.8888/		服以工作区-hy401-hy402-hy403	4.)
	http://10.3.0.8/49153/		WUA工作区-hg401-hg402	
	http://10.3.0.8:49167/		105以工作包-hy401-hy402	
			< 1 2 3 4	5 28 > 10条/页- 建亚 3

- 点击 "删除",可以删除在资产组列表里的目标主机资产和目标 Web 资产;
- 点击"提交"成功修改资产组。



3.4.4.4 自动类型资产组列表编辑

在资产组列表处,点击自动同步类型资产组的"编辑",即可打开编辑资产组界面(如下入所示):

* 资产组名称	测试1
备注	请输入备注
*所属组织单位	联认工作区
资产同步模式 ⑦	自动同步
* IP B9 ⑦	name × 02 × 02 × test() × test ×

具体操作如下:

- 可修改资产组名称,不能为空;
- 可修改备注内容;
- 所属组织单位和资产同步模式不可更改;
- IP 段可编辑,不能为空;
- 点击"提交"成功修改资产组。

3.4.5 资产属性管理-IP 段管理

在左侧导航栏中,选择"资产中心-资产属性管理-IP段管理",进入IP段管理界面:

此页面可以帮助企业的管理员对 IP 段进行管理,支持对 IP 段的增加,编辑,删除, 查询。

3.4.5.1 内容展示

该页面展示 IP 段的名称、具体段内容、负责人、所属组织单位等信息。用户可以 根据筛选条件筛选条目,添加、查看、编辑、删除条目

(1)调监。	0.02									admin
默认工作区	-юлт V	资产中心 / B	er metter / IP Re	ряц.						
② 全局仪表盘	1	(Million	R#位 默认工作区 ×	+ 添加等选条件						
日白橙管理	~	• E3	FF0个把段						O 批量操作	× + 添加 IP 段
』 基线管理	~					護论 IP				
小 铁像扫描	÷		IP 殺名称	IP段	负责人	数	实际存活 IP 数	存活更新时间	所属组织单位	操作
意 资产中心			测试	10.3.0.0/24	15	256	1	2024-06-28 18:21:40	默认工作区	-
资产全景									共1条 🕢 1	> 10 泰/页 >
资产列表	÷									
流产属性管理	~					-Ray XR-S(H) 10-24	06.001_r11 @ 2024 Cha	ilin Tech.		
PR10										
业务系统管1										
网络区域管理	r									
标签管理										
· 東府管理	~									
自 报表中心	~									
〇 知识库	~									

支持批量操作:



3.4.5.2 添加/编辑 IP 段

点击右侧"+添加 IP 段"添加新的 IP 段, 输入 IP 段名称, 以 10.0.0.1/24 的格式输入 IP 段/IP 段列表, 所属组织单位以及负责人信息保存

< < → 洞瑩 x-							tmin
默认工作区	×	現代中心 / 現代	周拉管理 / IP段管理	1	添加 IP 段		×
② 全局仪表盘		所属组织单位	】 默认工作区 ×	+ 源加筛选条件			
	*	0 已选择	0个IP段		基本内容		
a ana	*		IP 段名称	P段	* IP 段名称	清靖写 IP 段名称	
章 御产中心	*		02	111124	* IP 段	请输入IP段。格式为10.0.0.1/24。多个IP段换行输入	
前产全量				A tradice			
资产列表	÷		02	10,3.0.1/24			4
用产属性管理	*		4	10.1.1.1/24	- 55尾组织的位	94-1 T-APTO	
中段管理			1222	1.2.2.2/26	///weiter/in	MAN LIPIC	
业务系统管理			hyl01	10.3.0.5/30	IP 段描述		
网络区域管理	t		hy/02	10.3.0.8/31	负责人		
标签管理			hyl03	10.3.0.4/29			
a 展彩管理	~		IP段-输收	10.0.0.1/12			
① 指表中心	*		name	10.0.0/24			
						取消	定

3.4.5.3 删除 IP 段

点击"删除"条目删除 IP 段,并可以再二次提醒后删除

< →洞螢×	RAY						admin
默认工作区	\sim	资产中心 / 资产	常性管理 / IP段管理				
() istawa		一种服组织单位	就认工作区 × ; + 添加	/ 提示			
A MONT		0 已选择	0 个 IP 段	确定删除当前选中的 IP 段吗?			批量操作 × + 添加 IP-段
◎ 南产中心			IP 股名称		取消 健定	所属组织单位	操作
资产全量			02	1.1.1.1/24		默认工作区	
還产列表			02	10.3.0.1/24		默认工作区-hylD1	
至产属性管理	2		1	10.1.1.1/24	(#S)	默认工作区	
中段管理			1222	1.2.2.2/26		默认工作区	28 KM 80
业务系统管理	2.		hyl01	10.3.0.5/30	hyl01	默认工作区-hyl01	
10.00 (0.00)			hy102	10.3.0.8/31	hv/02	默认工作区-hvi01-hvi02	25 63 53
* #R###			hvi03	10.3.0.4/29	hvi03	联认工作区-hvi01-hvi02-bvi03	
·····································			IDEL MANY	10.0.0.1/12	admin	BULTING	
C sign				10.0.0.024	ANDINA	BRILT PETR	
② 系统管理	*		name	10.0.0.0.24		MMALIFIA	an ad an



3.4.5.4 查看 IP 段

点击"查看"条目查看 IP 段信息,包含 IP 段名称、描述、所属组织单位、负责人,IP 段信息等

支持查看每个 IP 段的理论 IP 数、实际存活 IP 数

< → 洞盟 x-											
默认工作区	~	nreo / F	的复数法律	管理				查看 IP 段			X
· 全商仪表盘	1	(MMH)	●位 默认工作区 ×	+ 激加骤送条件							
H IDENT	2	• E&	择口全护酸					基本内容			
4 25522	*					1840 (0		IP 程名称	测试		
华 获集扫描	÷.		IP 段名称	IP段	负责人	数	实现	IP 段描述	- 時以十進度		
\$ # # #0	~		30107	10.3.0.0/24		256	1	负责人	-		
资产全销								IP 段	理论 IP 数	实际存活 IP 数	
意作利用	*							10.3.0.0/24	256	1	
资产就当知道	*					X-Ray XR-504/10-24.04	1.0013				100
P 花香菇											فإناد
拉芬系统管理	E .										
网络区域管理	6										
杯放發理											
· 派羽银道	~										
	*										
	÷										

3.4.6 资产属性管理-业务系统管理

在左侧导航栏中,选择"资产中心-资产属性管理-业务系统管理",进入业务系统 管理界面。

3.4.6.1 内容展示

主要展示所有的业务系统名字(如下入所示):

	批量操作	▼ + 添加业务系
2011年11月1日 11日11日 11日11日 11日11日 11日11日 11日11日 11日11日	所属组织单位	操作
业业 医 前 1	请不要删除测试数据	编辑 影陆



3.4.6.2 业务系统操作

添加业务系统

- 在列表页点击"添加业务系统"按钮,显示填写内容的弹窗
- 注意:业务系统不能被重复添加。

* 业务系统名称:			
* 组织单位:	默认工作区	~]	

删除业务系统

● 批量/单次删除业务系统

■ 注意:如果业务系统正在被使用,那么该业务系统不允许被删除。

売戸中心 / 田介高伯領国 / 业务系统管理			
(NEWERSER X) + 通知課意条件			
● 已选择 0 个业务系统			批量操作 - 一 - 第10位考系统
总共查询到 0 美业务系统			8018
业务系统名称		所属组织单位	操作
	加天政部		
			< 0 > 10条/賞∨

编辑业务系统

● 点击列表页的"编辑"按钮,显示更改内容的弹窗:



编辑业务系统			×
* 业务系统名称:	业务系统1		
* 组织单位:	请不要删除测试数据	\sim	
		取消	确定



3.4.7 资产属性管理-网络区域管理

在左侧导航栏中,选择"资产中心-资产属性管理-网络区域管理",进入网络区域 管理界面。

3.4.7.1 内容展示

主要展示所有的网络区域名字:

(FERESEC 请不要删除测试数据 ×) + 添加算适条件			
已选择 0 个网络区域			批量操作 × + 加加网络区
8共查询到 0 条网络区域			
网络区域名称		托属组织单位	操作
	報天数部		

3.4.7.2 网络区域操作

添加网络区域

● 在列表页点击"添加网络区域"按钮,显示填写内容的弹窗:

67-16/10/1011年7月62月1日						
(HIXHSINE) 请不要根除测试数据 ×) + 透加研究条件	添加网络区域 🚽	-		×		
● 已选择 0 个网络区域	* 网络区域名称:					<u>就量操作 ~ </u>
网络区域名称	* 组织单位:	请不要删除责试数据			所属组织单位	16.17
			п и	确定		
						< 0 > 10条/双。



删除网络区域

● 批量/单次删除网络区域:

 中心 / 第一段15日 / 飛絡反域管理 (所現地が中区 病不要影説前ば数度 ×) + 添加資意条件 ● 已透明 0 个网络互通 			Indian
北共查询到()条网络区域 网络区域名称		所属组织单位	
	MARK.		

● 注意:如果网络区域正在被使用,那么该网络区域不允许被删除。

编辑网络区域

● 点击列表页的"编辑"按钮,显示更改内容的弹窗。

*网络区域名称:	测试		
* 组织单位:	请不要删除测试数据	v	

3.4.8 资产属性管理-标签管理

在左侧导航栏中,选择"资产中心-资产属性管理-标签管理",进入网络区域管理 界面:

3.4.8.1 内容展示

通10%装置環 制体造中的%況要律		
医囊腔积率位 默认工作区 X + 漆加等遗条件		
总共宣调到1条标签管理		
- 标签名称	所属組织拳位	操作
	默认工作区	san ma
		10.8/0



3.4.8.2 标签操作

添加标签

- 在列表页点击"添加标签"按钮,显示填写内容的弹窗:
- 注意:标签不能被重复添加。

CHG I REALER / SHEER				
(淡加标签管理	×		
0 EAR 0 198888	* 杨莹名称:			
日月登市213 市村当堂市	· 續明學位: 请不要删除测试数据			
1012.010			PERCENTION	NHTP.
		2.8 EX2	請予展剔時到任款價	1010 809
虚拟化策略模型			由不是他的形式放出	50 20
UTISHI			这个就是2012年1月	101 BOR
				4 10 m/g -

删除标签

- 批量/单次删除标签
- 注意:如果标签正在被使用,那么该标签不允许被删除。

(TETERATION AND A DESCRIPTION OF		
• 8.88	13 14 14 15 14 14 14 14 14 14 14 14 14 14 14 14 14		比較時代 > + 活成的医療目
	N258#	所属组织争位	18-17
	sb	派统法律师师不管	9610 B100
8	意知代謝總模板	请不要他协会试知识	6616 RTP
	(#1288)	请不要删除到试数册	stant state
			< 1 → 10条/页~

编辑标签

● 点击列表页的"编辑"按钮,显示更改内容的弹窗:

编辑标签管理			Х
*标签名称:	1		
* 组织单位:	默认工作区	~	
		取消	确定



3.5 漏洞管理

此模块主要提供对漏洞管理的功能,包括对漏洞的查询筛选、删除、漏洞状态的 跟踪更新等,方便企业对漏洞进行管理。

3.5.1 漏洞全景

在左侧导航栏中,选择"漏洞管理-漏洞全景",进入基线检查配置界面。

<・>洞鉴x	-RAY				admin
默认工作区	V 38	府世世 / 漏洞全景			
の 全局仪表盘					
日 扫描管理	~			满全现伊	些看面度: 款1A上1FE8,2023-04 选择数据常言面度
A 基线管理	~	漏洞总数		探測漏洞数③	
恋 液产中心	~		2698		2
☆ 漏洞管理	~	318	402 463 1515	1	2 0 0 0
3312B		环比增长率: 0.0%		来自1个资产	
濕洞列表					
圓 报表中心	*	待修复漏洞数	已修复漏洞数	新增漏洞	修复漏洞
🗋 知识库	~	2638	59	0	0
⑥ 系统管理	~	310 397 450 148	1 7 5 13 34	0 0 0	0 0 0
▲ 用户管理		高危及以上占比: 26.7%	平均漏洞修复时间 4 周 6 天 20 小时 57 分钟	环比增长率: 0.0%	环比增长率: 0.0%
		漏洞变化趋势			
		2800			◆ 至部 ◆ 做范 ◆ 甲范 ◆ 高范 ◆ 产重
		2100-			

此页面展示系统所有漏洞的统计信息,内容包括:

- 漏洞数量:
 - 漏洞数量:包含漏洞总数、待修复漏洞数量、已修复漏洞数量的数据,展示不同风险程度的漏洞数量(严重、高危、中危、低危);
 - 显示漏洞总数的环比增长率、高危及以上占比、平均漏洞修复时间;
 - 探测漏洞数量及来自的资产个数、新增漏洞及环比增长率、修复漏洞及环比增 长率。
- 漏洞变化趋势:
 - 最近十一次扫描的漏洞数量变化趋势;
 - 鼠标悬浮在图形上,会显示当前状态下的漏洞数量,包含(全部、严重、高危、
 中危、低危)。
- 漏洞修复状态统计



- 饼状图展示不同类型的漏洞分布情况,鼠标悬浮在饼图上会显示所选部分标识的漏洞类型、漏洞数量占比
- 数据展示不同漏洞类型的漏洞数量
- 修复漏洞耗费时间分布,主要展示修复不同风险程度的漏洞时,所耗费时间的 分布情况
- 未修复的漏洞数量,主要展示处于待修复状态下不同风险程度的漏洞数量



- 漏洞类型统计
 常见漏洞类型数量统计,鼠标悬浮显示漏洞、名称、数量、占比
- 弱口令统计
 - 显示弱口令名称、占比、排名、影响服务、弱口令数、影响资产数



- 业务系统漏洞分布情况
 - 显示排名、业务系统、漏洞总数、影响资产数
- 组织单位漏洞分布情况
 - 显示排名、组织单位、漏洞总数、影响资产数



业务系统漏洞分布情况						
			排名	业务系统	漏洞总数	影响资产数
	留无欺握				111元数册	
织单位漏洞分布情况						
			排名	组织单位	運調总数	影响资产数
1 默认工作区		100%	18	默认工作区	34414	326

3.5.2 漏洞列表

在左侧导航栏中,选择"漏洞管理-漏洞列表",进入漏洞列表界面。

3.5.2.1 漏洞列表

内容展示:

漏洞列表页面展示洞鉴扫描出的所有漏洞信息,展示内容包括漏洞等级、漏洞权重、 漏洞名称、存在漏洞的位置、负责人、漏洞状态、建议处理优先级、创建时间、最近发 现时间、漏洞的发现次数、操作栏,(如下图所示):

- 漏洞权重越高, 越确信漏洞的存在
- 建议处理优先级从 p0-p4, 优先级逐渐降低

242	(管理 /	漏洞列表								
	(HRE	织单位 默认工作	⊠ X) + 3	资加罪送条件						
	• B	选择 0 个漏洞						Gi	i洞髮测管理 1	は最操作 ~
		漏洞等级	漏洞权重	漏洞名称	存在漏洞的位置	负责人	漏洞状态处理	发现次数	建议处理优先级	创建时间
		**	99%	hyl-丝袜哥	http://10.3.0.208:8080/	admin	• 待分配 ~	1	PO	2023-03-1:
			99%	CVE-2019-070	10.3.0.206:3389/TCP	admin	● 待分配 ~	1	P0	2023-03-1:
		-	99%	CVE-2016-870	10.3.0.206:11211/TCP	admin	■ 待分配 ∨	1	P0	2023-03-1:
		-	9996	CVE-2016-870	10.3.0.206:11211/TCP	admin	• 待分配 ~	1	P0	2023-03-1:
		-	99%	CVE-2012-000	10.3.0.206:3389/TCP	admin	• 待分配 ~	1	P0	2023-03-1:
		F 0	99%	CVE-2015-750	http://10.3.0.8:49156/	admin	■ 待分配 ~	2	PO	2023-03-1:
		78	99%	CVE-2015-750	http://10.3.0.8:49153/	admin	• 待分配 ~	2	P0	2023-03-1:
		-				141			-	

筛选漏洞:

- 在列表页可对漏洞进行筛选操作,可根据漏洞名称、漏洞风险等级、漏洞确信程度、 相关资产、漏洞状态、发现时间、创建时间、相关扫描任务,自由添加一个或多个 条件进行筛选
 - 当选择"负责人"筛选条件时,可根据所选择的负责人进行多组筛选。

添加筛选条件		×
所属组织单位		
所属组织单位	组织单位不能为空	
负责人		
漏洞名称		
漏洞等级		取消保存
漏洞权重	http://tomcat-manager.vul.ct:8900/do adr	min ● 待分配 >
漏洞状态处理		
漏洞编号	http://tomcat-manager.vul.ct:8900/ adr	min ● 待分配 >
漏洞位置		
负责人	v hyl02 × ydy ×	
十	hyl01	
十 添加筛选条件	hyl01 hyl02	~
十 添加筛选条件	hyl01 hyl02 ydy	✓ ✓ { @ #
+ 添加筛选条件	hyl01 hyl02 ydy xiaoming	✓ ✓ ≰_保存
+ 添加师选条件	hyl01 hyl02 ydy xiaoming HYL02	✓ ✓ 分配>
+ 添加师选条件 detail测试	hyl01 hyl02 ydy xiaoming HYL02 chanpin02	✓ ✓ 分配 ✓
+ 添加师选条件 detail测试	hyl01 hyl02 ydy xiaoming HYL02 chanpin02 tht	✓ ✓ 分配 ✓ 分配 ✓

删除漏洞:

在列表页可以对漏洞进行批量删除,一旦执行了删除操作,所有选中的漏洞均将被 删除,具体操作说明如下:

- 选中要删除的漏洞,此时显示已选择的漏洞总数;
- 同时 "删除" 按钮变 为可点击状态;
- 点击"删除"按钮,提示框提示确定是否删除,点击"确定",则删除成功。



所属组	织单位 默认工作	X + 3	泰加筛选条件						
0 2	选择 1 个漏洞						C a	洞复测管理	批量操作。
÷	漏洞等级	漏洞权重	漏洞名称	存在漏洞的位置	负责人	漏洞状态处理	发现次数	建议处理优	删除 清空
	71	99%	hyl-丝袜哥	http://10.3.0.208;8080/	admin	■ 待分配 >>	1	PO	编辑状态 生成报表
	PB.	99%	CVE-2019-070	10.3.0.206:3389/TCP	admin	• 待分配 ~	1	PO	复测漏洞
	7°1	99%	CVE-2016-870	10.3.0.206:11211/TCP	admin	■ 待分配 >	1	P0	2023-0
	₩ E	99%	CVE-2016-870	10.3.0.206;11211/TCP	admin	■ 待分配 >	1	P0	2023-0
	(FE	99%	CVE-2012-000	10.3.0.206:3389/TCP	admin	■ 待分配 >>	1	P0	2023-0
	₽ ∎	99%	CVE-2015-750	http://10.3.0.8:49156/	admin	● 待分配 ~	2	P0	2023-0
	PB	99%	CVE-2015-750	http://10.3.0.8:49153/	admin	● 待分配 ∨	2	PO	2023-0

生成漏洞报表:

在漏洞列表页可以选择多个漏洞并生成漏洞报表,具体操作说明如下:

- 选中希望生成报表的漏洞,此时显示已选择的漏洞总数;
- 同时"生成报表"按钮变为可点击状态;
- 点击"生成报表"按钮;
- 在弹出的窗口中输入相关生成配置;
- 点击"确认",即可以开始生成所选漏洞的报表。
- 注:可以前往报表管理页面查看报表生成的情况,或下载生成好的报表。

(PEIME	组织单位 默认工作	x + 1	版加筛选条件						
0 E	3选择 1 个漏洞						© M	洞复测管理	批量操作 ~
	漏洞等级	漏洞权重	漏洞名称	存在漏洞的位置	负责人	漏洞状态处理	发现次数	建议处理优	删除 清空
	F	99%	hyl-丝袜哥	http://10.3.0.208:8080/	admin	● 待分配 ∨	1	PO	编辑状态 生成报表
	/*B	99%	CVE-2019-070	10.3.0.206:3389/TCP	admin	● 待分配 ∨	1	PO	复测漏洞
	/*∎	99%	CVE-2016-870	10.3.0.206:11211/TCP	admin	• 待分配 >	1	PO	2023-03-1
	(FE	99%	CVE-2016-870	10.3.0.206:11211/TCP	admin	● 待分配 ~	1	PO	2023-03-1
	F	99%	CVE-2012-000	10.3.0.206:3389/TCP	admin	● 待分配 >>	1	P0	2023-03-1
	FB	99%	CVE-2015-750	http://10.3.0.8:49156/	admin	● 待分配 ~	2	P0	2023-03-1
	μ.	99%	CVE-2015-750	http://10.3.0.8:49153/	admin	• 待分配 ~	2	PO	2023-03-1



成报表					
*报表名称:	CVE-2013-2251:ApacheStrute多个输入验证错误漏转的漏词报表				
*所属组织单位:	意识工作说				
*报表类型:	国用标志				
*报表模板:	漏洞报表模板				
*报表文件格式:	管理报表供账 12 Word 版 12 Excel 版 12 HTML 版 🗌 PDF 版				
* 目标漏消:	从漏游列表导入				清空已选目标
	名称	相关资产	所属组织单位	发现时间	操作
	CVE-2013-2251: Apache Struta 多个输入验证错误漏洞	http://s2-009.vul.ct:8184/	默认工作区	2021-12-21 17:06:07	818
					< 1
					_

复测选中漏洞:

在列表页可以对漏洞进行批量复测:

O Bi	选择 1 个漏洞						© #	洞复测管理	社量操作 ~
•	漏洞等级	漏洞权重	漏洞名称	存在漏洞的位置	负责人	漏洞状态处理	发现次数	建议处理优	制除 清空
	E1	99%	hyl-丝袜哥	http://10.3.0.208:8080/	admin	• 待分配 ~	1	PO	编辑状态 生成报表
	FB.	99%	CVE-2019-070	10.3.0.206:3389/TCP	admin	• 待分配 ~	1	PO	复测漏洞
	78	99%	CVE-2016-870	10.3.0.206:11211/TCP	admin	• 待分配 ~	1	PO	2023-03
	FE.	99%	CVE-2016-870	10.3.0.206:11211/TCP	admin	• 待分配 ~	1	P0	2023-03
	FB	99%	CVE-2012-000	10.3.0.206:3389/TCP	admin	● 待分配 >>	1	P0	2023-03
	FB	99%	CVE-2015-750	http://10.3.0.8:49156/	admin	● 待分配 ~	2	P0	2023-03
	-	99%	CVE-2015-750	http://10.3.0.8:49153/	admin	● 待分配 >	2	PO	2023-0

- 点击漏洞复测按钮,系统会针对该漏洞进行重放请求,漏洞复测通常用时较短,复 测中的漏洞不能停止,超出 1min 中后,将自动结束复测任务;
- 填写对应参数,需要注意,在不填写任何参数时,会直接按原有参数执行具体操作 说明如下。
 - 选中希望复测的漏洞,此时显示已选择的漏洞总数,同时"复测漏洞"按钮变为可点击状态;
 - 点击"复测漏洞"按钮
 - 在弹出的漏洞复测对话框中配置相应信息;



- 点击确定开始复测。
- 说明:漏洞验证仅支持验证漏洞权重大于75%的漏洞,系统将会默认复测您选中的漏洞中漏洞权重大于75%的漏洞。

)
漏洞复测仅支持漏 您选中的漏洞中漏 以下为复测参数 填写则会使用漏漏 修改	洞权重大于 75 的漏洞进行复测,系统将会默认复测 洞权重大于 75 的漏洞。 2置,填写后将覆盖漏洞检出时使用的配置参数。若不 刚检出时的特征信息。建议非必要环境下不进行参数的	
▼ HTTP 配置		
User-Agent		
cookie 参数 ⑦	uid_example=12345; Finger=abc; session=ABC	
	> 高级选项	
自定义请求头 ⑦	+ 增加一个新的自定义 HTTP 请求头	
HTTP 代理 ⑦		
▼ HTTPS 客户端证	书配置	
▼ HTTPS 客户端证 客户端证书文件	^{书配置}	
▼ HTTPS 客户端证 客户端证书文件	书配置 点击或将文件拖拽到这里上传 文件大小不超过 10 M	
HTTPS 客户端证 客户端证书文件 客户端证书密码	书配置 点击或将文件拖拽到这里上传 文件大小不超过 10 M	
 HTTPS 客户端证 客户端证书文件 客户端证书密码 客打平台配置 	书配置 点击或将文件拖拽到这里上传 文件大小不超过 10 M	
 HTTPS 客户端证 客户端证书文件 客户端证书密码 盲打平台配置 选择盲打平台 	市配置 点击或将文件拖拽到这里上传 文件大小不超过 10 M 内置盲打平台 >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	
 HTTPS 客户端证 客户端证书文件 客户端证书密码 盲打平台配置 选择盲打平台 	市配置 点击或将文件拖拽到这里上传 文件大小不超过 10 M 内置盲打平台 >	

更改漏洞状态:

- 漏洞状态包括待分配,验证中,修复中,误报,忽略,复核中,已修复,漏洞状态 会根据洞鉴扫描或管理员修改而变化;
- 洞鉴扫描发现的新漏洞, 会默认设置为"待分配"状态;

● 洞鉴扫描发现的已有漏洞,若已经在"待分配"、"验证中"、"修复中"、"复核中"、"误

报"、"忽略",则不会更新状态;

- 洞鉴扫描发现的已有漏洞,若已经设置为"已修复"状态,则重新设置为"待分配" 状态;
- 管理员可以对漏洞状态进行跟踪,手动修改漏洞状态(若变为已修复,则不可手动 更改)。
- 可以点击列表头批量调整漏洞状态来批量选中漏洞并调整漏洞的状态为任何目标 状态

所属组	眼单位 默认工作	x + 3	泰加筛送条件						
9 B	选择 2 个漏洞						G	漏洞复测管理	批量操作 >
	漏洞等级	漏洞权重	漏洞名称	存在漏洞的位置	负责人	漏洞状态处理	发现次数	请注意批量词 态 瑞议处理的	整状态后不可恢复原料
	/*#	99%	hyl-丝袜哥	http://10.3.0.208:8080/	admin	• 验证中 ~	1	P0	编辑状态 生成报表
	PE	99%	CVE-2019-070	10.3.0.206:3389/TCP	admin	• 待分配 ~	1	P0	复测漏洞
	#B	99%	CVE-2018-870	10.3.0.206:11211/TCP	admin	● 待分配 ~	1	P0	2023-03-1

所派組 • 日3	R单位 默认工作 选择 0 个漏洞	x) + 3	泰加筛选条件				C 1	洞复测管理 批	:量操作 ∨
	漏洞等级	漏洞权重	漏洞名称	存在漏洞的位置	负责人	漏洞状态处理	发现次数	建议处理优先级	创建时间
	-	99%	hyl-丝袜哥	http://10.3.0.208:8080/	admin	●驗证中♡	1	PO	2023-03-1:
	Fn	99%	CVE-2019-070	10.3.0.206:3389/TCP	admin	 待修复 误报 	1	P0	2023-03-1
	F#	99%	CVE-2016-870	10.3.0.206:11211/TCP	admin	 忽略 待分配 × 	1	PO	2023-03-1
	FE	99%	CVE-2016-870	10.3.0.206:11211/TCP	admin	• 待分配 >	1	PO	2023-03-1;
	P.B.	99%	CVE-2012-000	10.3.0.206:3389/TCP	admin	● 待分配 ∨	1	P0	2023-03-1:

3.5.2.2 漏洞详情

点击漏洞列表中的漏洞,可以打开漏洞详情页面,了解漏洞更多的相关信息和技术 细节:



CVE-2013-2251: Apache Struts 多个输入验证错误漏洞

技术细节		基础信息	
manin te	高兴用述 Apache Struls提美国阿帕奇(Apache)软件基金会的一个开意项目,是一套用于包建企业级Java Web应用的开意MVC框架,主	漏洞名称	CVE-2013-2251: Apache Struts 多个输入验证错误漏 洞
漏洞细节	要提供两个板本框架产品。Struts 1和Struts 2。Apache Struts 2.0.0至2.3.16版本中存在输入验证错误漏洞。远程攻击者可通过 带有action:, redirect:或redirectAction:的面服參数利用该漏洞执行任意OGNL表达式。	漏洞类型	其他
漏洞危害		漏网等级	2
CVSS 评分	國同語节 经过时以下目标进行扫描测试:	漏洞权置	99%
影响组件 影响范围	http://ś2-009.vul.ct:8184/AjaxRemoteForm.action	漏涡缩号	CT-24262 CVE-2013-2251 CNNVD-201307-306 6118 9
漏洞验证方式		所属资产	http://s2-009.vul.ct:8184/
修复方案	发现存在该漏洞。	影响资产类别	其它
調測短星	灑得探测过程的请求流为 第1个请求为	所属任务	浏览器隐虫test
	GET /AjaxRemoteForm.action?redirect:%24%7841124*44734%7D HTTP/1.1	发现时间	2021-12-21 17:06:07
	User-Agent: Mozilla/5.0 (Windows NT 10.0; MOW64) AppleWebKit/537.36 (KHTML, like Gecko) Cl	温炭状态处理	• 待分配 🗹
	Accept-Language: en-US Cookie: JSSSIONID-448E0E03143FCA548833A2A90E04F56E2 Referer: http://s2-009.vul.ct:8184/config-browser/showConfig.action?namespace=6actionName:	标题	原理台旗 WEB 漏洞 HW重点推测
	Accept-Encoding: gzip	处理过程	
	第1个编成为	○ 特分配 扫描发	2021-12-21 17:06:07
	HTTP/1.1 302 Content-Length: 0 Date: Tue, 21 Dec 2021 09:03:19 GMT Location: /1839641016		

基础信息:

漏洞详情右侧上方展示漏洞的基础信息。

- 漏洞名称:该漏洞名称
- 漏洞类型:该漏洞类型
- 漏洞等级:该漏洞等级,可手动修改
- 漏洞权重:权重越高,漏洞存在的可能性越大
- 漏洞编号:漏洞的 CVE、CNNVD 编号
- 所属资产:点击可跳转到该漏洞所在的资产详情页面(若license 中不包含资产管理模块或者无权限查看该模块则无此功能)
- 影响资产类别
- 最近扫描任务:点击可跳转到扫出该漏洞最近的一次扫描任务详情页面
- 发现时间:表示此漏洞在目标上扫描出来的时间
- 漏洞状态处理:可在此更改漏洞状态:
 - 点击漏洞状态右侧的"铅笔"图标,漏洞状态变为可操作的下拉菜单;
 - 在下拉菜单中点击新的漏洞状态,即可修改漏洞状态;
 - 若不想改变漏洞状态,点击右侧的"取消"即可退出对漏洞状态的更改。
- 处理过程:显示漏洞状态的发现或状态更新过程

技术细节:

漏洞详情页面左侧展示漏洞的技术细节信息。技术细节提供关于漏洞的详细的技术 支持,包含漏洞描述、漏洞危害等等。

● CVSS 风险评分:



- CVSS 是一个通用的漏洞风险评分系统, CVSS 评分可以表示该漏洞的风险 情况, 评分越高表示风险越高。
- CVE 类型介绍:
 - CVE 是一个通用的漏洞类型信息库。CVE 信息可以对漏洞形成的原因做一 个较好的补充说明;
 - 洞鉴系统仅节选一部分 CVE 类型介绍。如果用户希望获得更多信息,可以访

问 CVE 官网 (https://cve.mitre.org/),并搜索洞鉴系统提供的 CVE 编号

(形如 "CVE-119") 获取更多漏洞类型说明。

漏洞复测:

针对 POC 检测的漏洞支持漏洞复测:

	发现 type 的借为
	echo_based
	漏洞危害
建设持续	 攻击者可以通过命令注入漏洞执行任意命令直接获得服务器系统权限 次击者可以通过命令注入漏洞执行任意命令直接获得服务器系统权限
100 100 100 100	2. 成士者可以通过审专注入编阅进一步扩入攻击旗,对整个内网发起攻击
AD ICC-44-NR	CVSS 评分
(1000 (EQ)	智无
0000 1927	
ICAPAE1+	影响组件
影响范围	
属调验证方式	影响范围
修复方案	
漏涡验证	潮得验证方式
	在上述骤鸦详情中,发送了一个带有命令执行请义的 payload,若该 payload 得到执行,那么将会在响应中存在执行的结果。
	漏洞雙測
	容認万測 1 原展游在通过会会世境兼教业准用某场会会的专式支空球妇关业务
	1. 改重起光道过单寸折接罗数未购的水机带又到力站未来或用大量另 2. 肩膜由多错性对田户输入的曲数嵌合体性助验
	3. 过速或转义用户输入中的敏感宇符
	o PHP 程序可使用 escapeshellarg 函数进行转义
	◎ Python 程序可使用 subprocess.call 函数调用子进程
	4. 部署 Web 应用防火疝 可以避免受到命令注入漏洞的影响
	漏洞验证

- 下发漏洞验证任务:
 - 点击"漏洞复测"按钮,系统会针对该漏洞进行重放请求,漏洞复测通常用时
 较短,复测中的漏洞不能停止,超出 1min 中后,将自动结束复测任务;
 - 填写对应参数,如图,需要注意,在不填写任何参数时,会直接按原有参数执行。



漏洞复测仅支持 您选中的漏洞。 以下为复测参 填写则会使用。 修改	诗漏洞权重大于 75 的漏洞进行复测,系统将会默认复测 中漏洞权重大于 75 的漏洞。 数配置,填写后将覆盖漏洞检出时使用的配置参数。若不 属洞检出时的特征信息。建议非必要环境下不进行参数的
HTTP配置	
Jser-Agent	
cookie 参数 ⑦	uid_example=12345; Finger=abc; session=ABC
	> 高级选项
自定义请求头 ⑦	+ 增加一个新的自定义HTTP请求头
HTTP 代理 ⑦	
HTTPS客户端证	书配置
户端证书文件	_
户端证书文件	
户端证书文件	点击或将文件拖拽到这里上传
户端证书文件	点击或将文件拖拽到这里上传 文件大小不超过10M
户端证书文件	运 点击或将文件拖拽到这里上传 文件大小不超过10M 请输入正确的客户端证书文件
户端证书文件	运 点击或将文件拖拽到这里上传 文件大小不超过10M 请输入正确的客户端证书文件
户端证书文件	点击或将文件拖拽到这里上传 文件大小不超过10M请输入正确的客户端证书文件
户端证书文件 ;户端证书密码	点击或将文件拖拽到这里上传 文件大小不超过10M 请输入正确的客户端证书文件
户端证书文件 ;户端证书密码 • 盲打平台配置 选择盲打平台	定 点击或将文件拖拽到这里上传 文件大小不超过10M 请输入正确的客户端证书文件 请输入正确的客户端证书密码

• 验证结果显示:

■ 验证后的结果会在右侧,出现漏洞复测操作,并显示漏洞状态:



		基础信息	
建 料描述 演用细节	面对指述 命令注入漏洞,又规称为 Shell 命令注入漏洞,即 Command Injection,是指道过提交思意构造的参数破坏服有的奇令语句结构,从而达到执行思意系统奇令的目的。	識詞名称 調調受型 調調等級	通用命令注入漏洞 代码注入
潮洞危害 VSS 评分	漏沿街节 段过对以下目标进行扫描图试:	調用収量	09%
影响组件 影响范围	http://10.3.0.5:9020/vulnerabilities/exec/	所属资产	http://10.3.0.5.9020/
始证方式 倖复方案 漏洞验证	发现存在该集网。 重调存在的参数位置为 body,参数老枪为 ip 重利探测过程的请求说为 第 1 个课代为	影响直产类别 所属任务 发现时间	dwa-cookie 2021-12-16 14:59:17
	POST /vulnerabilities/exec/ HTTP/1.1 Host: 10.3.6.5:9920 User-Agent Hotill/5.6 (Windows NT 10.0; NOW54) AppleMebKit/537.36 (KHTML, like Gecko) Cl Content-Length: 55 Content-Length: 55	副詞状态处理 标签 外理计算	• 1977年(2017年) CMMARP.top10 原理目指 WEB 編用
	Cookie: PMPSESSID=udd&gbpc-dpd⊃()jnuog691; security=low Referer: http://l0.3.0.519020/vulnerabiliies/exec/ Accept-Encoding: grip Submit=SubmitEip==c+1+127.0.0.1%0Aesp+68/2048472+%28-999306220%0A	○ 特分配 副洞板 ○ 特分配 目描表)	圏 2021-12-27 14:33:38 夏 2021-12-16 14:59:17

- 漏洞复测管理
 - 点击"漏洞复测管理"按钮可对复测的漏洞管理任务进行查看,支持一键清空全部复测记录。
 - 将漏洞的最近一次复测结果同步显示到漏洞列表中,"已下线"表示对应的服务 或端口已被关闭则复测。

	漏洞						C MA	夏朝管理 - Rt	遺操作 ~
- 漏洞等	级 漏洞权重	漏洞名称	存在漏洞的位置	负责	ы	漏洞状态处理 发	现次数	建议处理优先级	创建时间
PB	99%	hyl-丝袜哥	http://10.3.0.208:8080/	adn	nin	• 验证中 V 1		P0	2023-03-
72	99%	CVE-2019-070	10.3.0.206:3389/TCP	adn	nin	● 待分配 ∨ 1		P0	2023-03-
	99%	CVE-2016-870	10.3.0.206:11211/TCP	adn	nin	● 待分配 ~ 1		PO	2023-03-1
洞夏周官埋								×	
可以对正在	复测的过程进行手动暂住	停。"已下线"表示对应的服务或如	省口已被关闭则复测,"复测失别	、 表示引擎未读取到	到响应结果。				
							清空全部记	*	
漏洞等级	漏洞名称	存在漏洞的位置	漏洞状态处理	复测状态	复测结果	复测时间	操作		
兩位	基础备份文件	http://10.3.0.5:8100/www.zip	 已修复 	复测结束	确认修复	2023-04-14 11:36:18	RRAN B	15 余利	
兩危	基础备份文件	http://10.3.0.5:8100/1.tar.gz	• 已修复	复测结束	确认修复	2023-04-14 11:36:18	-	5188	
48	基础临时文件	http://10.3.0.5:8100/.DS_Stor	9 • 已修复	复测结束	确认修复	2023-04-14 11:36:18	-	時間記	
910	基础系统文件	http://10.3.0.5:8100/.ssh/knor	wn_hosts ● 已修复	复测结束	确认修复	2023-04-14 11:36:18		國務 记	
THE.	基础测试文件	http://10.3.0.5:8100/vendor/a	ompose ● 已修复	复测结束	确认修复	2023-04-14 11:36:18	-	5.68	
98	基础临时文件	http://10.3.0.5:8100/a.out	 已修复 	复测结束	确认修复	2023-04-14 11:36:18	-	51818	
中意	基础管理后台	http://10.3.0.5:8100/admin/	 已修复 	复测结束	确认修复	2023-04-14 11:36:18	-	5680	
中度	基础系统文件	http://10.3.0.5:8100/.vimrc	• 已修复	复测结束	确认修复	2023-04-14 11:36:18	-	5100	
	基础测试文件	http://10.3.0.5:8100/debug.tx	t • 已修复	复测结束	确认修复	2023-04-14 11:36:18	-	Sim	
Ф.E.									

3.6 报表中心

报表中心主要用于对洞鉴生成的报表和报表模版进行管理,包括报表管理和报表模版。

3.6.1 报表管理

在左侧导航栏中,选择"报表中心-报表管理",进入报表管理界面。

默认工作区	~	表中心 / 报表管理							
◎ 全局仪表盘			E作区 ×) + 添加筛选条件						
日 扫描管理	×	● 已选择 0 个报	R					批量操作、	+ 生成报表
⊿ 基场管理	•	1 秋态	报表名称	报表类型	报表语言	所属组织单位	报表生成时间	报表完成时间	报表下载
\$ 资产中心	~								
△ 漏洞管理	Ψ.	 已完成 	testzzz	资产报表	中文	默认工作区	2023-11-29 18:30:02	2023-11-29 18:30:05	
直 报表中心	•	 已完成 	test-split=zz	资产报表	中文	默认工作区	2023-11-29 18:29:14	2023-11-29 18:29:17	
服務管理		 已完成 	10.9.34.70的资产报表	资产报表	中文	默认工作区	2023-11-29 18:27:58	2023-11-29 18:28:01	
报表模拟		 已完成 	测试	资产报表	中文	默认工作区	2023-11-27 16:43:18	2023-11-27 16:43:22	
C MIRA	×	 已完成 	10.3.0.9的资产报表	资产报表	中文	默认工作区	2023-11-27 14:29:06	2023-11-27 14:29:08	
ひ 所所留理 A 用户管理		 已完成 	hyl-丝袜哥_hw、hyl-丝袜哥	漏沟报表	中文	默认工作区	2023-11-27 14:10:02	2023-11-27 14:10:08	
		 已完成 	明吧明吧	漏洞报表	中文	默认工作区	2023-11-24 17:52:44	2023-11-24 17:52:44	B
		已完成	测试来源	扫描任务报表	中文	默认工作区	2023-11-20 18:00:43	2023-11-20 18:00:46	
		 已完成 	雷池漏洞报告	漏洞报表	中文	默认工作区	2023-11-13 11:02:26	2023-11-13 11:02:28	

3.6.1.1 内容展示

报告列表页展示生成的所有报告,内容包括生成状态、报告名称、报表类型、报表 语言、所属工作区、报告生成时间、可下载的报表文件:



-	114 0 1 1845	1 month, i within the Manager and Alexandra an							Constant of
	状态	报表名称	报表类型	报表语言	所属组织单位	报表生成时间	报表下载	操作]
	• 已完成	OWASP-benchmark的扫描任务报表	扫描任务报表	中文	默认工作区	2021-12-20 16:46:46		28	2018
	• 已完成	OWASP-Benchmark的扫描任务报表	扫描任务报表	中文	默认工作区	2021-12-20 16:45:34		皇翁	2019
	• 已完成	test1	扫描任务报表	中文	默认工作区	2021-12-20 14:12:06		24	-
	 已完成 	https://192.166.50.13:8443/benchmark的扫描任务报表3	扫描任务报表	中文	默认工作区	2021-12-20 14:11:27		删除	
	• 已完成	https://192.168.50.13:8443/benchmark的扫描任务报表2	扫描任务报表	中文	默认工作区	2021-12-20 14:10:37		#172	
	 已完成 	https://192.168.50.13:8443/benchmark的扫描任务报表	扫描任务报表	中文	默认工作区	2021-12-20 14:09:54		28	an is
	 已完成 	https://182.168.50.13.8443/benchmark的扫描任务报表-资产视角	扫描任务报表	中文	默认工作区	2021-12-20 13:47:26		删除	
	 已完成 	https://192.168.50.13:8443/benchmark的扫描任务报表	扫描任务规表	中文	默认工作区	2021-12-20 13:47:09		删除	
	• 已完成	SSH顾口令篇调的漏踪报表	漏洞报表	中文	默认工作区	2021-12-13 11:46:19		24	me.
	• 已完成	SSH窗口令漏洞的漏洞报表	漏洞报表	中文	默认工作区	2021-12-13 11:45:43		요리	100

3.6.1.2 筛选操作

在报告列表页可对报告进行筛选操作,可根据生成状态、报告名称、报告类型和报告生成时间,自由添加一个或多个条件进行筛选

报表名称	~	请输入要筛选的内容	模糊匹配>	
+ 添加筛选条件	4			


3.6.1.3 下载操作

在"报表下载"列,会展示生成报表时勾选的文件格式(共有 word、html、Excel、 PDF、JSON),若生成的为英文版则显示左上角带有 EN 标识的 icon。

HTML	DOCX	XLSX	PDF
HTML	DOCX	XLSX	PDF

- 图标为较透明的彩色:表明对应格式的文件正在生成;
- 图标为彩色:表明对应格式的文件已生成,点击可下载;
- 图标为灰色:表明对应格式的文件已生成。

在报告列表页可以批量下载报告,具体操作为:

- 选中要下载的报告,此时显示已选择的报告总数,同时"下载选中的报告"按钮变为可点击状态;
- 点击"下载选中的报告"按钮,选择要下载的报告格式,点击确定后以 zip 的形式 将所有选择的报告下载到本地,文件包含选择的要下载的文件格式。

(Jinga	的单位 默认工	作区 × + 酒加游送条件						
0 B	选择 3 个报表	下载造中的报表 删除造中的报表						+ 生成服務
	状态	报表名称	报表类型	报表语言	所属组织单位	报表生成时间	报表下载	操作
	• 已完成	test22223	漏洞报表	英文	赋认工作区	2021-12-06 19:10:24	a a a	和新 新建
	 已完成 	trest111111	扫描任务报表	英文	默认工作区	2021-12-06 18:07:51	-	重載 删除
	• 已完成	【2021-12-06_17:51:41】 test1扫描报表	扫描任务报表	中文	默认工作区	2021-12-06 17:52:38	dana -	登載 删除
	 已完成 	qq	源网报表	英文	默认工作(8	2021-12-06 15:12:43		意味 副标



3.6.1.4 查看操作

12.00		经机管理									
	IT BEAD	用原的 數以工	作起 ×								
	0 E3	8種 0 个报表							批算時行 ッ	+ 4	成报表
		105	摇表名称	报表类型	报表语言	所属组织单位	报表生成时间	报表下数		勝作	
		• 巴克战	荔坞142	基线检查报表	中文	假以工作区	2023-07-11 16:27:20			#194	
		• 已完成	12345	基线检查报表	中文	默认工作区	2023-07-11 11:47:55		- B- B-	8.10	
1		* 日完成	1的任务对比报表	任务时比报表	中文	默认工作区	2023-06-27 14:13:02		6		813
		• 已完成	1的任务对比报表	任务时让报表	中文	默认工作区	2023-06-27 14:12:45		5	28	HEF8
		* 已完成	担归资产对比报表	资产对出报表	中文	默认工作区	2023-05-05 20:53:37			-	813
		 已完成 	医归对比据离	任务对出报表	中文	默认工作区	2023-05-05 20:53:18	88	-		80

报表生成 html 格式成功后,可点击"查看"按钮在线查看生成的报表。

3.6.1.5 删除操作

在报告列表页可以对报告进行批量删除,一旦执行了删除操作,所有选中的报告信 息均将被删除且不能恢复,具体操作为:

2 全局仪表盘		(mas	1999年位 默认工	作区 ×) + 添加筛选条件									
日描修理	*	0 E	选择 10 个报	R						批量操作 ∨	+	生成报	ŧ
(基线管理	÷		状态	报表名称	报表类型	报表语言	所属组织单位	报表生成时间	报表完成	制除	报表下	st.	
资产中心 漏洞管理	× .		 已完成 	testzzzz	资产报表	中文	赋认工作区	2023-11-29 18:30:02	2023-11-2	9 18:30:05			2
报表中心	^		 已完成 	test-split=zz	资产报表	中文	默认工作区	2023-11-29 18:29:14	2023-11-2	9 18:29:17		B	1
报表管理			• 已完成	10.9.34.70的资产报表	资产报表	中文	默认工作区	2023-11-29 18:27:58	2023-11-2	9 18:28:01	₽		1
报表模板			 已完成 	测试	资产报表	中文	默认工作区	2023-11-27 16:43:18	2023-11-2	7 16:43:22			IST
知识库	2		 已完成 	10.3.0.9的资产报表	资产报表	中文	默认工作区	2023-11-27 14:29:06	2023-11-2	7 14:29:08			
用户管理	×		• 已完成	hyl-丝袜哥_hw、hyl-丝袜哥…	潮洞报表	中文	默认工作区	2023-11-27 14:10:02	2023-11-2	7 14:10:08			à
			• 已完成	1910219102	漏洞报表	中文	默认工作区	2023-11-24 17:52:44	2023-11-2	4 17:52:44			
			 已完成 	测试来源	扫描任务报表	中文	默认工作区	2023-11-20 18:00:43	2023-11-2	0 18:00:46			
			 已完成 	雷池漏洞报告	漏洞报表	中文	默认工作区	2023-11-13 11:02:26	2023-11-1	3 11:02:28	D		2



3.6.2 生成报表

在报告管理可以生成报告,具体操作为:

- 从报告列表页点击"+生成报告"按钮,打开弹窗;
- 填写报告名称;
- 选择所属组织单位;
- 选择报告类型,包括扫描任务报表、基线检查报表、资产报表、漏洞报表四种类型
- 根据报告类型的不同,需要设置的内容也不同,每种报告模板对应的设置说明如下:

扫描任务报表:

● 报表模版:可选项为"扫描任务报表"下的模版;系统模板默认只生成漏洞权重大

于 50%的漏洞信息,如需更改请使用自定义模版。

- 点击"管理相关模版"可打开模版管理页面,对相关模版进行管理;
- 报表文件格式: 勾选要生成的文件格式;
- 报表处理:
 - 按资产聚合:扫描任务的漏洞将以所属资产的维度呈现;
 - 按漏洞聚合:扫描任务的漏洞将以漏洞种类的维度呈现;
- 拆分子报表:报表目标数量过多时建议选择拆分模式拆分为多个报表,避免单个报 表打不开等异常问题
- 报表目标: 点击按钮可选择目标扫描任务, 支持选择多个扫描任务。
- 全部设置好后,点击"确定",则成功生成报告,系统自动跳转至报告管理页;
 - "合并生成": 多个任务结果输出 1 份报表
 - "批量生成": 多个任务结果输出多份报表
- 可在报告列表页对刚生成的报告进行查看、下载和删除。



•报表名称:					
* 所属组织单位:	默认工作区				
*报表类型:	扫描任务报表				
* 报表模板:	扫描任务报表模板				
* 报表文件格式:	管理报表模板 Word 版 S Excel	版 🔽 HTML版 🗌 PDF版			
报表处理:	● 按资产聚合 ○ 按	漏洞聚合			
* 目标扫描任务:	点击选择目标扫描任务	ğ			清空已选目
* 目标扫描任务:	点击选择目标扫描任约 扫描任务	所屬组织单位	扫描启动时间	扫描状态	清空已选目
* 目标扫描任务:	点击选择目标扫描任5 扫描任务	所属组织单位	扫描启动时间	扫描状态	清空已选目 操作
* 目标扫描任务:	点击选择目标扫描任约 扫描任务	所属组织单位	扫描启动时间 ————————————————————————————————————	扫描状态	清空已选目 操作
* 目标扫描任务:	点击选择目标扫描任约 扫描任务	所属组织单位	扫描启动时间 ————————————————————————————————————	扫描状态	清空已送日 操作
* 目标扫描任务:	点击选择目标扫描任约 扫描任务	所属组织单位	扫描启动时间	扫描状态	操作

选择目	标扫描任务					×
扫描任	务:	扫描启动时间:	开始日期 ~	結束日期 □		
所闖釒	组织单位: 默认工作区	扫描状态:				
-	扫描任务			所属组织单位	最近扫描时间	扫描状态
-	Test			默认工作区	2023-03-13 14:17:54	② 扫描结束 (成功)
	 Test 实例1 			默认工作区	2023-03-13 14:17:54	扫描结束 (成功)
					< 1	> 10 条/页 ∨
	hostfor白名单v3-kai			默认工作区	2023-03-13 14:16:29	 扫描结束 (成功)
	hostfor白名单v3-kai 实例1			默认工作区	2023-03-13 14:16:29	② 扫描结束 (成功)
	hostfor白名单v3-kai 实例2			默认工作区	2023-03-10 18:21:18	② 扫描结束 (成功)
	hostfor白名单v3-kai 实例3			默认工作区	2023-03-10 18:19:33	🕑 扫描结束 (手动结束)
					< 1	> 10条/页∨
+	webfor白名单v3-kai			默认工作区	2023-03-13 14:16:24	ⓒ 扫描结束 (成功)
+	v3 深度服务			默认工作区	2023-03-13 14:16:25	 扫描结束 (成功)
+	深度web			默认工作区	2023-03-10 17:56:38	⊘ 扫描结束 (手动结束)
+	testhttp			默认工作区	2023-01-11 16:20:55	⊘ 扫描结束 (手动结束)
+	http://10.9.33.32:8080			默认工作区	2023-01-17 18:32:35	② 扫描结束 (成功)
+	1			默认工作区	2023-01-09 17:33:12	⊘ 扫描结束 (手动结束)
+	hang-test			默认工作区		



资产报表:

- 报表模版:可选项为"资产报表"下的模版:系统模板默认只生成漏洞权重大于 50%的漏洞信息,如需更改请使用自定义模版。
 - 点击"管理相关模版"可打开模版管理页面,对相关模版进行管理;
- 报表文件格式: 勾选要生成的文件格式;
- 报表目标:点击按钮可选择目标资产:资产组、Web 站点资产和主机资产;
- 全部设置好后,点击 "确定",则成功生成报告,系统自动跳转至报告管理页;
- 可在报告列表页对刚生成的报告进行查看、下载和删除。

生成报表				×
*报表名称	R:			
* 所属组织单位	立: 默认工作区			
* 报表类型	2: 资产报表			v
* 报表模板	5: 资产报表模板			
* 报表文件格式	t: 💟 Word 版 💟 Excel 版 💟 HTML 版	PDF 版		
* 报表目标	ត: ● 主机和 Web 站点 🔵 资产组			
	选择目标主机			清空已逃目标
	资产地址	所價组织单位	标签	操作
		腦无数線		
	选择目标 Web 站点			潮空已选目标
	资产地址	所属组织单位	标签	操作
				取消确定

漏洞报表:

报表模版:可选项为"漏洞报表"下的模版;系统模板默认只生成漏洞权重大于 50%的漏洞信息,如需更改请使用自定义模版。



- 点击"管理相关模版"可打开模版管理页面,对相关模版进行管理;
- 报表文件格式: 勾选要生成的文件格式;
- 报表目标:点击按钮可选择目标漏洞;
- 全部设置好后,点击 "确定",则成功生成报告,系统自动跳转至报告管理页;
- 可在报告列表页对刚生成的报告进行查看、下载和删除。

生成报表						×
* 报表名称:						
* 所属组织单位:	默认工作区					×
* 报表类型:	潮洞报表					×.
*报表模板:	漏洞报表模板					
* 报表文件格式:	管理报表模板 I Word 版 I Excel 和	🖌 HTML版 🗌 PDF版				
* 目标灑淵:	从漏洞列表导入					清空已选目标
	名称	相关资产	所属组织单位		发现时间	操作
				<u></u>		
						取消 前定

基线检查报表:

- 报表模版:可选项为"基线检查报表"下的模版;
 - 点击"管理相关模版"可打开模版管理页面,对相关模版进行管理;
- 报表文件格式:勾选要生成的文件格式;
- 报表处理:
 - 按资产聚合:基线检查的结果将检查资产的维度呈现;
 - 按检查策略聚合:基线检查的结果将以检查策略的维度呈现;
 - 提示:若检查的主机数量较多,可能会导致相同检查项被重复打印多次,导致
 生成报告内容过多;建议选择"按检查策略聚合"。
- 报表目标:点击按钮可选择目标基线检查;
- 全部设置好后,点击 "确定",则成功生成报告,系统自动跳转至报告管理页;



● 可在报告列表页对刚生成的报告进行查看、下载和删除。

- ALIAN					
* 服表名称:					
* 所属组织单位:	默认工作区				
* 报表类型:	基线检查报表				
* 服表模板:	基线检查报表模板				
*报表文件格式:	Word Ri C Excel Ri	🛃 HTML 🕅 🗌 PDF 🎉			
报表处理:	一 投资产聚合 () 按检查	2前略聚合			
* 目标检查任务:	点击选择目标检查任务				滞空已选择机
	检查任务	所属组织单位	扫描启动时间	任务状态	操作
			加无数据		
			加无联曲		
			加无抑度		



3.6.3 报表模版

在左侧导航栏中,选择"报表中心-报表模版",进入报表管理界面。

<・>洞鉴×	-RAY					admin
默认工作区	× 1	青中心 / 报表模板				
② 全局仪表盘		扫描任务报表 基线检查报表	资产报表 漏洞报表	任务对比报表 资产对比报表		
□ 扫描管理	*	所展组织单位 默认工作区 ×	+ 添加筛选条件			
总 基线管理	×					
志 资产中心	~	模板名称	描述	创理单位	模板来源	操作
0 運用管理		资产对比报表模板	系统内置默认模板	8	内置模板	
· 报表中心	^					< 1 > 10条/页∨
报表管理						
经收税机	1			X-Rey XR-S(H) 10-23.03.001, r15 (0 2022 Challin Tech.		
□ 知识度						
③ 系统管理	~					
△ 用户管理	*					

3.6.3.1 内容展示

扫描任务报表、基线检查报表、资产报表、漏洞报表、任务对比报表、资产对比报表。这 6 种类型的报表对应模版差异较大,可通过顶部 tab 页面切换。

在报表模版中,展示已有模版的模版名称、描述、模版来源:

- 模版来源:系统出产自带的为"内置模版",其余均为"自定义模版";
- 内置模版仅可查看,不可编辑和删除;
- "自定义模版"可以点击操作列的按钮,查看、编辑和删除。

3.6.3.2 筛选操作

在报告模版页可对报告进行筛选操作,可所属组织单位、模版名称、模版来源维度
 筛选,自由添加一个或多个条件进行筛选。

3.6.3.3 添加报表模版

- 选择报表类型:目前只支持扫描任务报表、基线检查报表、资产报表和漏洞报表。
 不同类型的报表,可勾选的内容、可筛选的标准有所不同;
- 模版名称:同类型的报表模版名称不可有重复;
- 报表语言:支持中文和英文版两种报表语言,默认为中文。选择该模版的报表生成 后将会是对应的语言;
- 报表封面标题:最终显示到报表封面的标题,如果不填写则默认显示报表名称;
- 描述;



- 模版创建单位:选择工作区;
- 模版内容: 勾选组合想要在报表中展示的内容模块;
- 数据筛选:对生成报告的初始数据进行筛选过滤,不同的报表模版类型有不同的数据筛选项。包含资产/漏洞风险等级、漏洞权重、资产类型、资产存活性、漏洞标签等筛选项

扫描任务报表	V
模板名称不能为空	
Ψχ	
	b
默认工作区	
 ● 該述信息 ● 资产结果统计 ● 资产结果统计 ● 资产风险分布 ● 操作系统统计 ● 服务类型统计 ● Web 框架分布统计 ● Web 框架分布统计 ● 风险结果统计 ● 選派风险分布 	
	 扫描任务报表 螺板名称不能为空 中文



3.7 知识库

3.7.1 漏洞库

在左侧导航栏中,选择"知识库-漏洞库",进入漏洞库界面。

显示当前漏洞库中漏洞相关的信息:

<→洞⊮×	RAY						admin
默认工作区	× .)	NRM / RRM					
① 全局仪表盘		接示:编码最新的得报信息请述反"编码被属时间"进行转选重用					
HERE	Υ.	+ 18,507118,85.19					
#WRA N	*	● 已选择 ◎ 今篇頁 此至下回任务 开级激讯库					
意 直产中心	1	二 画用名称	漏洞等级	B1221318	影响相伴	影响资产类别 标签	操作
= 3639€4	1						
章 編成中心	*	CVE-2021-30918. Apple PadOS安全部制	E	8	-		重視 影明图作 +
व अस्तव	-	CVE-2021-30874: Apple IOS 安全漏洞		æ	65	324	建度 影明图广 ~
884		CVE-2021-30894: Apple txO5 超冲区错误重要	63	25	1		
首志义 POC	_	□ CVII-2021-30892: Apple macOS Big Sur皮全運用	-	8	14	(4)	
02.589		CvE-2021-30817: Apple 多股产品输入验证错误漏洞	-	5	14	83)	55 8488/* ~
Ф ж л ян		CVE-2021-30886: Apple tvOS 安全雇用	-	8	02	120 120	
A. 南戶營稽	۰ ۳ ۰	CvE-3021-30854: Apple IvOS 权限许可和边间控制问题漏离	-	西	5 1		28 5857 v
		CVE-2021-30855: Apple macOS Big Sur 銀冲区證说圖明		西			
		CVE-2021-30881: Apple tvO5 输入给证错误漏消	-	. 22	24		京者 影响图7***
		CVE-2021-30898: Apple macOS Big Sur 竞争条件问题漏洞		25			索相 医时进产 >
						(1 2 3 4 5 ···· 16647 >	10 \$//5 < NE

3.7.1.1 列表内容

- 漏洞名称
- 漏洞等级:包括严重、高危、中危、低危
- 原理扫描:包含是/否
- 影响组件
- 影响资产类别
- 标签:为漏洞添加的标签

3.7.1.2 添加筛选条件

可以通过添加筛选条件,包含漏洞名称、等级、编号、影响组件、服务类型、操作 系统、标签、厂商、是否需要反连、漏洞类型、影响资产类别、是否原理扫描、漏洞披 露时间、自定义标签:

- 添加筛选条件可以选择后保存,或者删除;
- 可以在列表上点击删除删除已经设定的筛选条件。



3.7.1.3 批量下发任务

● 点击全选或者单个选中漏洞项目,点击批量下发任务,进行任务的扫描:

	JURN N											
mas	回半位 數认工作	E X + 1	查加排选条件									_
0 B	选择 10 个运用									G (80	RANGE REP	10 v
	2482	RRGR	漏洞名称	存在漏洞的位置	负责人	建用状态处理	最近和测结束	发现次数	建议处理优先级	19580PE/A	新花和18月 湯空	
		99%	CVE-2023-218	10.3.0.5.7206/TCP	admin	* 已修复	明认修复	2	P0	2023-04-21 15:11:40	2023-0-21 編版5 生成系	(市) (市)
	-	00%	CVE-2023-218	10.3.0.203:7001/TCP	admin	•已修复	输认维度	1	<i>P</i> 0	2023-04-21 15:11:04	2023-0-21	10
	60	99%	CVE-2023-218	10.3.0.5:7201/TCP	admin	• 時分配 ~	022	1	P0	2023-04-21 15:10:47	2023-04-21 15:10:4	7
•		99%	CVE-2023-218	10.3.0.5:7206/TCP	admin	• 特分配 ~	0.00	1	P0	2023-04-21 15:10:31	2023-04-21 15:10:3	5 E
		99%	CVE-2023-218	10.3.0.5:7208/TCP	admin	• 11940 -	12.5	1	P0	2023-04-21 15:10:17	2023-04-21 15:10:1	7 🛢
2	63	99%	CVE 2023-218	10.3.0.202:7001/TCP	admin	• 1898E ~		1	P0	2023-04-21 15:10:01	2023-04-21 15:10:0	•
		99%	CVE-2023-218	10.3.0.5.7202/TCP	admin	● 特分配 ~	(191) (191)	3	P0	2029-04-21 15:09:47	2023-04-21 15:09:4	7
8	60	99%	CVE-2020-148	10.3.0.5:7291/TCP	admin	* (8:982 ×	*	2	P0	2023-04-21 10:15:23	2023-04-21 15 11/0	0
	633	99%	CVE-2020-148	10.3.0.5:7201/TCP	admin	●特分配 ~	1960	2	P0	2023-04-21 10:15:22	2023-04-21 15:10:5	9
	633	9996	CVE-2020-148	10.3.0.5:7201/TCP	admin	• 10 G B2 ~	100	2	P0	2023-04-21 10:15:21	2023-04-21 15:10:5	8 🔳

- 当以选中漏洞批量创建扫描任务时,创建的扫描任务名称会自动变为:"任务名称+
 所在组织单位名称",同主机资产下发扫描任务。
- 3.7.1.4 升级漏洞库

详情请见 4.3.2 漏洞库升级。

3.7.1.5 自定义标签

支持给漏洞库自定义标签,自定义标签支持在扫描任务/扫描策略中筛选对应的漏 洞插件。

3.7.1.6 查看详情

- 点击查看,进入漏洞情况页面:
- 包含漏洞名称、风险等级、标签、影响资产类别、漏洞类型、是否原理扫描、漏洞
 概述、漏洞编号、漏洞披露时间、漏洞危害、CVSS 评分、影响组件、影响范围、
 修复方案、影响资产数量以及漏洞近一周、一月、一年的漏洞趋势。



< → 洞巖 x-						admin
跌认工作区	v					
② 全向仪表盘		CVE-2021-45428: Te	elesquare TLR-2005KSH 安全漏洞 🇮			
目接管理						
6 高档管理		63日	题理日前 Network Devices	#R200	近一個 近一日 近半年	
き 図广中心	٣	影响资产类别	操作系统	4		
a second		潮洞失望	其他	3		
		應理約續	#	2		
章 振表中心	*	星月極述	Telesquare Tir-2005Kah是韩国Telesquare公司的一款 Sk 电讯 Lte 路由器。 T	1	0	
anna C	*		elesquare TLR-2005KSH 存在安全漏洞,该漏洞当于 TLR-2005KSH 受不正 确的访问控制漏洞影响。 启用 PLIT 方法,因此攻击者可以上传任意文件,包	0 mean	DEBINE MEINE MEISE MERSE	
8.004			括 HTML 和 CGI 格式。		 → 漏洞出現頻次 	
BIER POC		定用编号	CT-224076 CVE-2821-45428			
			CNVD-2822-04552			
自定义指纹			CNWVD-202201-074			
≥ 系统繁確		混词披露时间	2022-01-03 00:00:00			
用户管理		漏洞危害	可能造成造成信息过篇,业务系统不稳定等安全问题			
		CVSS 风险评分	9,8			
		MINTER	tir-2005ksh_firmware			
		影响范围	影朝經件版本不時識			
		律复力案	建议尽快得某安全问题,并做好安全管理工作,定期进行安全活地,最大现 废地避免安全问题。			
		影响目标就量	11			

3.7.1.7 其他操作

点击影响资产,选择主机资产或者 Web 资产跳转到对应影响的资产详情页面。

3.7.2 自定义 POC

在左侧导航栏中,选择"知识库-自定义 POC",进入自定义 POC 界面。

< ⋅> 洞罂 x	-RAY					ədmin
默认工作区	v	HILL DEEX POC				
① 全用仪表章		+ 淡加绿流条件				+ IEta (SZÉK POC
S COUNT	4	展明名称	莱森等级	重音证明	16 M	18/1
计单位管理		d1818	(CO)	d d		
○ 運動装施 二 第5440	*	1	-	i i		10.76 St.46 Matte 2013
日 御倉中心	v.					(1))10条/页~
C sas				X-044-30-0	0 IN YOM HER DON'T Chaine Team	
2005						
BIER POO						
自定义服机						
◎ 系統管理						
令 相合器理	- 20					

权限说明:

● 该功能需要具备"扫描管理"功能模块的 license,详细请联系长亭工作人员获取;



超级管理员支持编辑和可见权限,系统管理员仅有可见和使用权限。

3.7.2.1 自定义 POC 列表-内容展示

自定义 POC 列表展示系统中所有自定义 POC 列表,列表包含漏洞名称、漏洞等级、漏洞类型、漏洞编号、标签。

+ 添加筛选条件				+ 漆加自定义 POC
瀛洞名称	漏洞等级	温润详情	标签	級作
山谷等		d d		1238 12240 14448 18818
t.	-	1		检测 重機 编辑 删除
				< 1 > 10条/页▽

3.7.2.2 筛选操作

在列表页可对任务进行筛选操作,可根据扫描漏洞名称、风险等级、漏洞编号、标签。

漏洞名称	~ 请转	俞入要筛选的内容	模糊匹配>	
+ 添加筛选条件	+			

3.7.2.3 删除操作

在列表页可以对单条 POC 进行删除操作,一旦执行删除操作,对应 POC 均将被 删除,会影响启用了该 POC 的任务配置,具体步骤为:

● 找到列表中要删除的扫描任务,点击尾部操作栏中的"删除"按钮。

+ 添加筛选条件				+ 漆加自定义 PC
灑洞名称	漏洞等级	漏洞详情	标签	38-f5
d等等		d d		检测 查看 编辑 图称
t.		r.		检测 靈機 编辑 删除
				< 1 > 10条/页



3.7.2.4 查看 POC 操作

在列表页可以对单条 POC 进行查看操作,具体步骤为:

● 找到列表中要查看的扫描任务, 点击尾部操作栏中的"查看"按钮。

+ 添加筛选条件				+ 添加自定义 POC
灑洞名称	漏洞等级	温润详情	标签	经作
山等等		d d		检测量量量 编辑 删除
1	-	1		检测 靈機 编辑 删除
				く 1 > 10条/斑マ

3.7.2.5 添加自定义 POC

添加 POC 可以手动添加或者上传文件。

+ 添加筛选条件				+ 源加自定义 POC
還洞名称	漏洞等级	漏洞详情	标签	級作
山谷谷	-	d d		检测 整制 编辑 删释
r		<u>f</u>		检测 重機 编辑 删除
				く 1 > 10条/頂×

手动添加:

- 点击"添加自定义 POC"按钮,选择手动添加,填写对应的漏洞模板,然后在下面的代码编辑器中,粘贴对应的检测脚本或按照脚本说明编写相应的检测脚本;
 - 漏洞模板--包含漏洞相关的静态描述字段,包括漏洞名称、漏洞类型、风险等级、漏洞编号、漏洞概述、漏洞危害、漏洞 CVSS 信息、漏洞修复方式以及标签;
 - 检测脚本--包含漏洞的检测脚本 yaml 格式,用户可以根据提示的编写规则粘 贴或编写对应的脚本。在代码编辑器下,可以点击跳转详细的《洞鉴 yaml 格 式自定义 POC 说明》。



* 漏洞名称	请输入规则名称	
* 瀘洞类型	请选择最限类型	
* 漏洞等级	请选择氟需等级	
漏洞编号	请集写时后的课程编号,例如 CVE-2018-2315,CNVD-2018-1015, 以证号分解	4
* 漏洞概述	诸狼入風雨極送	
• 逼须危害	博输入展现危害	- le le
漏洞 CVSS 信息	请输入服用 CVSS 信息	le
修复方案	領输入修复方案	
		4

桐签	+ 桐匪
* 检测脚本	1 4 初间:
	2 # 順本現職內得得描述明: https://z-ray-test.in.chaitin.net/task/poc/description
	3 # FOT 服本中包含 3 个错;
	4 # set: ()string
	\$ # miler: (]Rule
	♦ # detail: nup(string)string.
	● # vuln_class 为自能义安重,当不堪写时,系统会自动填写新认信,以下是变量名代表的复数
	9 # title 是 编词名称 (不读写刻)使用name, 填写刻(使用此名字)
	10 # category 建 属积类型 (不堪写默认为阈色)
	11 # security 是 風羽谷田 (不現写影以为中意)
	12 # verbose_name R MRM-9
	13 · # numary 是 周阳极近
	14 / impact # MANDAN
	15 / cran & MillerardBS
	16 f solution 道 作取方案
	17 / tagn 是 标准 (新创建的标准规认为遗色)
	18
	19 并 name 是 题明名称 (企坊)
	20 # set 是用来自定义更量。比如是随机数、反连平台等
	63 host_infor
	64 hostname: "test"
	65 e Martin
	66 vulnerability:
	67 id: "秋亭寨湖岸 id"
	68 match: "证明重得存在的信息"
	69 # 其它学校
	70 eve: "cvE-2020-1234"
	71 # 氯它未用個從文的字程
	72 summary: "test"
2	73
	脚本编写详细说明,请参考《篇册 yami 植式自定义 POC 说明》
	取消 健交



上传文件

- 点击自定义 POC,选择从文件夹上传;
- 导入根据文件模版写成的.yml 格式的文件, 点击确定添加。

批量添加 POC	×
点击下载文件模板	
₽	
点击或将文件拖拽到这里上传 文件大小不超过 5 M;文件类型:.yml	
取消	确定

3.7.2.7 编辑自定义 POC

在列表页可以对单条 POC 进行编辑操作,具体步骤为:

- 找到列表中要查看的扫描任务,点击尾部操作栏中的编辑按钮,进入漏洞编辑页面;
- 填写对应的漏洞模板,然后在下面的代码编辑器中,粘贴对应的检测脚本或按照脚本说明编写相应的检测脚本。
 - 漏洞模板--包含漏洞相关的静态描述字段,包括漏洞名称、漏洞类型、风险等级、漏洞编号、漏洞概述、漏洞危害、漏洞 CVSS 信息、漏洞修复方式以及标签;
 - 检测脚本一包含漏洞的检测脚本 yaml 格式,用户可以根据提示的编写规则粘贴或编写对应的脚本。在代码编辑器下,可以点击跳转详细的《洞鉴 yaml 格式自定义 POC 说明》。



说明:编辑后的漏洞模板在进行新的任务检测后,新的字段会批量覆盖到之前与该漏洞模板关联的漏洞。

+ 添加筛选条件				+ 漆加自定义 POC
灑洞名称	漏洞等级	漏洞详情	标签	接作
d等等	-	d d		162701 102-102 102100 BH110
t		r.		检测 查報 编辑 删除
				< 1 > 10 条/页 >

3.7.2.8 自定义 POC 快速检测

在列表页可以对单条 POC 进行检测操作,具体步骤为:

- 找到列表中要查看的扫描任务,点击尾部操作栏中的检测按钮,进入 web 漏洞检测任务下发流程;
- 默认插件选择仅有自定义 POC 对应的插件。

+ 添加筛选条件				+ 潮加目定义 POC
漏洞名称	運用等级	漏洞详情	标签	经作
山谷寺		dd		检测 查看 编辑 删除
1	-	<u>f</u>		检测 建模 编辑 删除
				< 1 5 10条/页マ

<→洞鉴×				admin
默认工作区	V.	1111年(《名书》書 / 通知扫描任务		
* *****		· · · · · · · · · · · · · · · · · · ·		
1 ISBN BIR	- 8	article instant mentalest		
5 基础管理	×	任务信息		
「第十年の	8			
1 MART		日識策略名称	基础 Web 满羽归相	
〒接着中心	~	扫描策略模型	5	
2 mar	~	日接筆勝自动首步 ①		
315.00				
BER POC		* 扫描任务名称 ①		
0225802		前注		
◎ 米代展理	*	* 日接日接	学动输入 上價料和文件 网络资产能	
6. 用户管理	*		EDB 1988 H.d. Hep://1.2.3.4V Hep://1.2.4.VEDP/Hews.UNde-1 Hep://www.undetti.cov	
		* 执行类型	23998	
		推定时间段 ①	· 指定于当地时间 面定常行的问题	
			Matalia 🕘 🕱 tatania	
			#20.579/#3	
			(KEW)在5.5 (MIR # 1	立即扫描任务



3.7.3 自定义指纹

在左侧导航栏中,选择"知识库-自定义指纹",进入自定义指纹界面。

-RAY						admin
×	ellil年 / 自定文指纹					
						+ 漆如日定义指纹
*	指纹名称	产品名称	厂商名称	关联演调数量	标签	操作
<i></i>						
*				留天森總		
8						< ○ > 10 象/页 ✓
				X-Rey XR-510 21, 11,001, 210 (2021 Challer	TRich.	
~						
<u>ې</u>						
		-RAY	-RAY	-RAY ▼ 1939 / BEX082 RXX 8/R	-RAY	RXX NUMB / BEX.RBX File File RXX BR File File File

- 3.7.3.1 自定义指纹列表
- 显示指纹信息,包含指纹名称、产品名称、厂商名称、标签(如下图):
- 可以查看、删除、编辑自定义指纹。
- 可以通过指纹名称、厂商名称、产品名称筛选自定义指纹

anish drifts	*8.49			40.00	+ 添加局定义指纹
指纹名称	产品名称	厂商名称	关联漏消数量	杨瓷	操作
			102.元3018		
					< 0 > 10 条/页 ∨

3.7.3.2 添加自定义指纹

- 点击添加自定义指纹,进入模版添加指纹名称、产品名称、检测 yaml 脚本
- 填写指纹名称、脚本中可输入指纹的 cpe, 版本, 描述等信息, 点击提交保存



<・>洞鉴 x	-RAY			admin
默认工作区	V	知识库 / 自定文指纹 / 添加自定:	2指纹	
⑦ 全局仪表盘		* 指纹名称	價驗入環控來施	
□ 扫描管理	~			
A 基线管理	w.	* 检测脚本	1 # 聪明:	
意 资产中心	~		2	
命 漏洞管理	*		3 # HHX 服本中主要包括以下键: 4 # rules: Limite	
◎ 报表中心	~		5 ≠ detail: map(string)string	
口 知识库	^		6	
漏洞库			7 # name 是 指纹名称 (必項)	
			8 # rules 是一个由规则 (Rule) 组成的列表, 后面会描述如何解写 Rule, 并将其组成 rules,	
BEX POG			9 # detail 是一个慷慨对,内部存储需要返回并表示的内容,如果无需返回内容,可以忽略。	
自定义指纹			10 # 详情请咨询长率科技相关工作人员	
©	*		11	
△ 用户管理	÷		12 name: fingerprint-yaml-http-	
			13 transport: http	
			14 rules:	
			15 《第一条rula的名字	
			16 ml:	
			17 # rule 開展包含 request 部分	
			18 request:	

<・>洞鉴×	-RAY		admin
默认工作区	×	如同师 / 自定义指纹 / 添加自定义指纹	
◎ 全局仪表量		30 # 定义如何限缩规则结果判断结果	
□ 扫描管理	*	31 expression: r1() r2()	
⊿ 基线管理	*	32 # detail倍很多填	
意 黄产中心	٣	33 detail: 24 《可读语写作者是谁	
◎ 漏洞管理	Ŷ	35 author: test	
□ 报表中心	*	36 # 自定义指纹的主要指纹信息、必须	
🖾 如识度	^	37 fingerprint:	
進羽库		38 infos:	
自定文 POC		39 # 如无别外, type 均方web服务对应 web_application, 其中name和cpe字段至少填写一个,其余参数选辑	
日定义接续		40 - type: web_application	
		41 name: canal # 指纹对应服务的名称	
◎ 系统管理	~	42 cpet ** # 指纹对应的标准 cpe, 可法律写, 如不填即使用 name, type, 和version字段作为指纹显示标准	
△ 用户管理	~	43 version: '' # 指纹对应的版本	
		44 confidence: 32 # 相纹置信度	
		45 description: '' # 油纹的相关描述, 可选	
		46	
		m中等中当中3m20月,销量等《Imply Sami 检测自定义值2000月》	
		取消	援交

四、系统管理介绍

4.1 系统设置

4.1.1 基本配置

在左侧导航栏中,选择"系统管理-系统配置",默认进入基本配置界面。

<·> 洞鉴x-	RAY						admin
默认工作区	V	「抗管理 / 系统设置					
の 全局仪表盘		基本配置 显示配]	1				
日 扫描管理	~			2022			
创 基线管理	~	登录策略配置		編輯《收起》	数据备份设置		編輯 收起
◎ 資产中心	~	登录超时时长①	3小时 0分钟		自动备份频率	每周	
☆ 漏洞管理	÷	操作超时时长①	1小时 0分钟			周一	
富 招表中心	~	登录时间窗判定①	3分钟		自动备份时间	11:18:04	
[™] win≉		最大登录重试次数	5				
	-	並來天政受限無TF 報告时间限制	银花赋亏 5分钟		FTP 服务器设置		编辑 收起
◎ 系机管理	~	账户重复登录限制①	禁用		10.45 Million		
系统设置					成分積減減加	- 21	
系统信息					工作模式	主动模式	
系统服务		密码策略配置		编辑 收起	用户名	-	
日志管理		密码最小长度限制	8				
引擎管理		密码更换频率	0天				
◎ 用户管理	~	密码复杂度设置	二級		日志仔順配直		福祥 收起
					存储上限设置	日志存储数量	
		SMTP 服务器配置		编辑 收起	日志留存时间	无限制	
					日志存储数量	不限	

基本配置包含登陆策略配置、密码策略配置、日志相关配置数据备份设置、FTP 服 务器设置、日志存储配置、访问 IP 限制等,每个模块的配置点击右上角"编辑"可进行修 改。



4.1.1.1 登录策略配置

对登录机制进行设置:

- 登录超时时长:登录超时设置,用户单次登录时长超过设置的时间,账号会自动登出,需要重新登录,默认3个小时,系统保留超时日志。
- 操作超时时长:操作超时设置,用户单次登录中超过设置时间未进行点击操作后, 账号自动登出,需要重新登录,默认1个小时,不可设置0数值,系统保留超时日 志。

admin 10.6.6.199 超级管理员 admin 操作超时,强制退出 2023-06-16 11:09:40

- 登陆时间窗判定:设定一段时长,在此时间内达到了最大登录重试次数,将触发受限,默认3分钟;
- 最大登录重试次数:登录系统时,账号和密码的连续尝试次数,默认5次;
- 登录失败受限操作:设置当连续登陆失败达到最大重试次数时,触发的受限,默认 锁定账号,可选项为:

■ 不限制;

- 锁定账号,一段时间后自动解锁:该用户账户状态变更为"锁定",期间可由
 管理员手动解锁,或到期自动解锁;锁定时长可在下方"锁定时间限制"中设置。
- 锁定 IP,一段时间后自动解锁:该登陆 IP 地址进入【访问 IP 限制】-【被锁定 IP】,期间可由管理员手动解锁,或到期自动解锁;锁定时长可在下方"锁定时间限制"中设置。
- 锁定时间限制:因登陆失败达到最大重试次数而触发的锁定账户或 IP 的锁定时长, 默认 5 分钟;
- 账户重复登录限制:默认为关闭。若开启,则在同一时刻,一个帐户仅能在一个 IP
 地址登陆,若在第二个 IP 地址登陆,会强制退出前一个 IP 的登陆。



● 登录验证码限制:默认为关闭。若开启,在登录界面会要求输入验证码。

用户登录	
A.用户名	
△ 田純	
0 man wt52	
£ 2	
如后记语码,请教系企业系统管理员或北京长亭未来科技 有效公司相关技术支持负责人寻求帮助	
	用户登录 A 用户名 B 密码 D 密 D 密

3-Ray 3R-5(H) 10-24.03.001_r9 @ 2024 Chaitin Tech.



4.1.1.2 密码策略配置

- 密码最小长度限制:设置用户账户密码长度的最小值,默认8位,在添加或编辑用
 户时,账户密码长度需大干等于最小长度;
- 密码更换频率:如果当前密码的使用时长达到设置的时间上限,没有做任何更改,那么再次登录时,必须按照向导先进行修改密码操作,才可查看并使用系统功能; 默认无限制;
- 密码复杂度设置:选择密码复杂度级别,默认二级,各级别对应以下要求:
 - 一级:至少包含大写字母、小写字母、数字、特殊字符中的任意1种字符;
 - 二级:至少包含大写字母、小写字母、数字、特殊字符中的任意2种字符;
 - 三级:至少包含大写字母、小写字母、数字、特殊字符中的任意3种字符;
 - 四级:同时包含大写字母、小写字母、数字、特殊字符。

4.1.1.3 SMTP 服务器设置

简单邮件传输协议(SMTP)是一种发送、接收邮件的标准协议。SMTP 配置页面可以帮助用户配置 SMTP 服务器。成功配置 SMTP 后,用户可以使用扫描结束后接收邮件通知的功能。

配置 SMTP

若用户还没有配置过 SMTP 服务器,在此处可以进行 SMTP 的配置,具体操作如下:

- 点击右上角 "编辑",显示 SMTP 配置的弹窗;
- 在弹窗中根据文案提示,配置相应信息;
 - SMTP 服务器:用户决定用来发送邮件的服务器地址 如:smtp.gmail.com;
 - 端口: 该服务器提供 SMTP 服务的端口;
 - ◆ 如:465

■ 发件邮箱账号:认证 SMTP 服务器所需的用户名;

◆ 如: xiaoming.li@gmail.com

- 发件人名称:将显示在用户收到的通知邮件"发件人"中,用户可以自行定义; 若此处为空,则系统默认以【显示配置】中的"产品名称"字段值作为发件人 名称;
- 连接授权码: 认证 SMTP 服务器所需的密码;
- 加密方式: 该服务器端口所使用的加密方式, 默认不加密;
- 邮件签名:邮件签名将显示在用户收到的通知邮件中,用户可以自行定义;
- 点击"保存",即可保存填写的 SMTP 配置。

内容展示

配置完成后,页面展示 SMTP 配置信息,包括服务器和端口、发件邮箱账号、发件人名称、邮箱签名。

测试 SMTP 发件配置

用户可在此处测试 SMTP 是否成功配置:

- 在"测试 SMTP 发件配置"处,填写收件测试邮箱的地址;
- 点击"开始测试"



SMTP 服务器配量	<u></u>	编辑收起
SMTP 服务器	smtp.163.com:25	
发件邮箱帐号	17343051504@163.com	
发件人名称	dfsdfdsfds	
加密方式	不加密	
邮件签名	dfsdfllllxiaxia	
收件测试邮箱		开始测试
)

打开上文填写的收件测试邮箱,若能收到来自发件邮箱的通知邮件,则证明 SMTP
 配置成功

😑 🎽 Gmail	Q、 搜索邮件	•	0 🕸 🏢	± 1990	1
+ 写邮件			第1个合话。共87个	$\langle \rangle$	
- 邮件	【长亭洞鉴】邮件通知配置成功通知 wmmx			• 2	0
□ 收件箱	长亭凋鉴 <17343051504@163.com>		下午5.08(0分钟前) 🟠	÷ :	
☆ 已加星标	发送里 轶 •				
③ 已延后					
▶ 已发邮件					+
□ 草稿	2				
✓ 显示更多标签					
• 会议	Let whe MD (Let us a surgery HP) (DB with mar VD down				
田 发起新会议	长亭洞釜 SMIP 配直成切通知				
我的会议	22 W AT 1				
	· 如善地:				
	如果您能收到此邮件,说明长亭洞器 SMTP 配置成功。				
	长亭科技				
	← 回复 → 特定				
					>



4.1.1.4 日志输出配置

可配置 syslog 服务器, 配置成功后, 本系统操作日志将自动传输至 syslog 服务器。

- 日志输出内容:当前仅支持输出全部内容;
- SYSLOG 服务器: 输入服务器和端口;
- RFC:选择数据格式规范协议,支持 RFC3164 或 RFC5424;
- 协议:支持 TCP 或 UDP。

4.1.1.5 数据备份配置

可开启自动备份并设置自动备份的周期和时间。

- 自动备份频率:可选择备份频率,每周、每月或自定义天数;默认不开启自动备份;
- 自动备份时间:开启自动备份后,设置具体的备份时间点。

4.1.1.6 FTP 服务器设置

此处仅配置 FTP, 后续将可将报告上传至配置的 FTP 服务器。

- 服务器地址;
- 端口号, 默认 21;
- 工作模式:可选主动模式或被动模式;
- 用户名:用户名为空则表示以匿名方式登陆;
- 密码: 以匿名方式登陆无需输入密码。

4.1.1.7 日志存储配置

- 存储上限设置:可选择按时间或者按数量对存储的日志进行限制;
- 日志留存时间:若选择按时间对日志存储进行限制,则选择日志的保留时间;超过 留存时间的日志将自动从数据库中移除;
- 日志存储数量:若选择按数量对日志存储进行限制,则设置系统最大存储的日志条数,默认不限;
- 达到上限告警通知:填写告警邮箱,当快达到设置的存储上限时,会给出邮件告警通知:



- 该功能使用的前提: 必须已成功配置 SMTP(详情见 3.1.1 基本配置–SMTP 服 务器设置)。
- 4.1.1.8 访问 IP 限制

对访问洞鉴系统的 IP 地址以黑名单或白名单进行限制。

- 限制方式:选择开启黑名单或白名单,对可访问系统的 IP 进行限制;
- 访问黑名单:在黑名单内的 IP 不可访问系统;输入支持 CIDR 和单个 IP 地址;各
 IP 间之间用换行隔开;支持 ipv6 和 ipv4;
- 访问白名单:仅在白名单内的 IP 可访问系统;输入支持 CIDR 和单个 IP 地址;各
 IP 间之间用换行隔开;支持 ipv6 和 ipv4;
- 被锁定 IP:展示因登陆失败达最大次数触发的被锁定 IP 列表;可手动对该 IP 进行 解锁,或等待锁定时间结束后, IP 自动解锁。

4.1.1.9 报表设置

- 报表生成超时时长:生成报表时若超过该设定值,报表生成将被判定为失败;默认两小时。
- 4.1.1.10 时间服务配置
- 系统时间:设置系统时间
- 是否同步:
 - 启用则每 30 秒通过 ntp 服务器同步一次时间;
 - 关闭则不同步时间,且不需要设置 ntp 服务器。
- ntp 服务器:当同步开启时,输入 ntp 服务器地址。
- 注:NTP 服务器时间配置能力仅支持硬件版。



4.1.2 显示配置

在上方分栏中,选择"显示配置",进入显示配置界面。

<->洞罂×	-RAY				admin
默认工作区	×	平式計畫 / 系统设置			
◎ 全局仪表盘		基本配置 服務	「記畫」 网络記言		
8 1969 1	*				
A 基线管理	<i>.</i>	系统显示配置 ①			-
\$ <u>R</u> ^++0	×	公司總称	北东长率未来科技有限公司	Notions (St)	
* 2 6883	$^{\times}$	产品名称	长亭四釜(X-Play)安全评估系统	型后于系统界图左上角阳报表(HTML)	
由 根表中心		产品型专	高级版	50000000000000000000000000000000000000	
a waw	×	页图形描	X-Ray XR-S10	上市于导出的局面 (1) 10 四年	
◎ 系統管理		板权信息	© 2021 Chaltin Tech.	X / PPI # A*RAY	
五机设置		技术支持邮箱	support@chaitin.com	2203 sogn 任憲副持 出示于所有編表	
系统信息		技术支持电话	400-032-7707	CHAITN	
系统服务		室网络转标题	长亭科技官网		
日志管理		宮网綿結 URL	https://ohaitin.or/		
引擎管理		帮助中心總維短篇	长亭科技帮助中心		
○ 局产管理	×	帮助中心器转 URL	https://aupport.chaitin.cn/		
				X-Rey XR-610.21.11.201 ; /10 @ 3021 Chadin Tech.	

支持企业对系统界面进行 OEM 配置,包含公司名称、产品名称、系统 Logo 等字段。



● 点击"系统显示配置"后的"问号"图标,可展开各配置项的影响位置说明。

《筑显示配直可帮助企业》	步行 OEM 配直,合配直坝目的影响位直如下表:
配置项	显示位置
公司名称	系统信息页、自定义 POC 表单、忘记密码等提示性文字
产品名称	系统信息页、报表、自动发送邮件
产品型号	系统信息页
页脚前缀	页面页脚
版权信息	页面页脚
技术支持邮箱	系统信息页、报表封面说明
技术支持电话	系统信息页
官网跳转标题	登录页面、报错页面、远程协助页面、上传证书页面
官网跳转 URL	登录页面、报错页面、远程协助页面、上传证书页面
帮助中心跳转标题	登录页面、报错页面、远程协助页面、上传证书页面
帮助中心跳转 URL	登录页面、报错页面、远程协助页面、上传证书页面
系统 Logo(浅色)	系统界面、报表(HTML)
系统 Logo(深色)	报表标题
公司 Logo	所有报表页眉



● 点击右上角的"编辑"按钮,可对显示配置的各项进行编辑

编辑系统显示 ⑦		×
* 公司名称	北京长亭未来科技有限公司	
* 产品名称	长亭洞鉴(X-Ray)安全评估系统	
* 产品型号	高级版	
* 页脚前缀	X-Ray XR-S10	
*版权信息 ⑦	© 2021 Chaitin Tech.	
* 技术支持邮箱	support@chaitin.com	
* 技术支持电话	400-032-7707	
* 官网跳转标题	长亭科技官网	
* 官网跳转 URL	https://chaitin.cn/	
* 帮助中心跳转标题	长亭科技帮助中心	
* 帮助中心跳转 URL	https://support.chaitin.cn/	
* 系统 Logo(浅色)	+ 上传	
	取消	定



4.2 系统信息

4.2.1基本信息

在左侧导航栏中,选择"系统管理-系统信息",默认进入基本信息界面。

<・> 洞鉴x	-RAY			admin
默认工作区	V	RETUR / REGIS	1	
◎ 全局仪表面		基本信息	试去拉拉 服务状态	
日白杨紫理	*			
A 基化管理	<i></i>	产品信息		
素 荒产中心	×	产品名称	长亭湖堇 (X-Ray) 安全评估系统	
* M02H	\sim	产品型号	商级版	
山 根表中心		系统版本	21.11.001_r10	
a waa	×	許可証信息		
© 系統管理	್	被握权单位	测试Icense申请	上傳動作可任
原約設置		证书状态	可用	
68.92		接权时间	2021-05-10 起 2022-05-11 止	
系统服务		当前43.0099	VXTM-SS44-XIOJ-XT07	点击或将文件拖拽到这里上传
日志管理		接权机器码	不限制	文件大小干面过 10 M
引擎管理		播权功能	扫描管理 治产管理	
○ 展示管理	*		漏洞管理 基线管理	
		授权曰道	基础 Web 展明扫描 基础服务展现扫描 结石资产发展 特定服务扫描 转达 Web 扫描 代理) 转达 Web 扫描 行志) 逻辑属明扫描	

包含产品信息、许可证信息和技术支持信息

4.2.1.1 产品信息

展示洞鉴的产品全称、当前产品型号、当前系统版本

产品信息				
产品名称	长亭调瓷(X-Ray)安全评估系统			
产品型号	高级版			
系统版本	21.11.001_r10			



4.2.1.2 许可证信息

展示信息:

许可证信息页面展示企业的许可证信息,内容包括以下字段:

- 被授权的企业名称
- 证书状态:证书到期前 30 天,会开始倒数提示证书还有多少天到期
- 授权时间
- 当前机器码
- 授权机器码
- 授权功能
 - 不同 license 版本具有不同的产品功能,详情可以联系对接您的长亭技术支持 同事
- 授权扫描
 - 授权扫描包括各类扫描策略
- 最大并发任务数
 - 决定了该产品最大可同时并发执行的任务数量上限(不限任务类型)
- 最大引擎节点数
 - 决定管理平台可连接的引擎数量上限

上传/更新许可证

在许可证信息页面,可对即将过期的许可证进行更换,具体操作如下:

- 在上传新许可证的地方,点击或将许可证文件拖拽到此处上传:
 - 点击红色区域,弹出文件框,选择许可证文件并点击确认,完成许可证的上传;
 - 直接将许可证文件拖到红色框选区域,也可完成许可证的上传。



	inter and	
授权单位)) 別山山icense中頃	上傳新许可证
中状态	可用	
要权时间	2021-05-10 起 2022-05-11 止	
自然机器码	VXTM-SS44-XIOJ-XTO7	点击或将文件拖拽到这里上
权机器码	不限制	文件大小不超过 10 M
災功艙	扫描管理 资产管理 漏词管理 基线管理	
反 权曰道	基础 Web 選択行語 基础 Web 選択行語 ա名 20 m X 30 主机 20 m 20	
a大井发任务数	10	

上传正确的许可证文件后,会显示被授权企业名称与授权使用时间。管理员确认无误后,点击"确认",即可完成许可证的更新,此时许可证内容显示新上传的许可证信息。

授权使用时间 2020-08-28 - 2021-08-29 当前机器码 一键复制 授权机器码 不限制 授权功能 扫描管理 最大并发任务数 10 最大引擎节点数 4 授权扫描 基础 Web 濾明扫描 基础服务漏洞扫描	被授权企业名称	长亭洞鉴测试-基础版
当前机器码 一键复制 授权机器码 不限制 授权功能 扫描管理 最大并发任务数 10 最大引擎节点数 4 授权扫描 基础 Web 漏洞扫描	授权使用时间	2020-08-28 - 2021-08-29
授权机器码 不限制 授权功能 扫描管理 最大并发任务数 10 最大引擎节点数 4 授权扫描 基础 Web 濡洞扫描 基础服务漏洞扫描	当前机器码	一键复制
授权功能 扫描管理 最大并发任务数 10 最大引擎节点数 4 授权扫描 基础 Web 漏洞扫描 基础服务漏洞扫描	授权机器码	不跟制
 最大并发任务数 10 最大引擎节点数 4 授权扫描 基础 Web 漏洞扫描 基础服务漏洞扫描 	授权功能	扫描管理
最大引擎节点数 4 授权扫描 基础 Web 漏洞扫描 基础服务漏洞扫描	最大并发任务数	10
授权扫描 基础 Web 漏洞扫描 基础服务漏洞扫描	最大引擎节点数	4
	授权扫描	基础 Web 漏洞扫描 基础服务漏洞扫描



4.2.1.3 技术支持

展示技术支持邮箱和技术支持电话

若用户遇到了产品使用手册上无法解决的问题,可以通过技术支持邮箱和技术支持
 电话,向长亭科技的技术支持人员求助。

4.2.2 状态监控

在上方分栏中,选择"状态监控",进入状态监控界面。

展示系统的整体运行状态,如下图所示:

<->洞罂 _{X-RAY}			admin
默认工作区 🗸 🗸	声的说道 <i>:</i> 系统信息		
② 全局仪表盘	基本信息 状态监控 服务状态		
日 10回登場 ~			
小 基线装置 ~	Sources Sources		
● 別 ⁴ 中心 ~	基本状态		
·	系统运行状态 正驚		
◎ 接着中心 ~	系統計詞 2022-01-04 17:13:43 ヹ 高統治行时分 AB5.5₹ 1/\8f 47分钟		
С жиж ~			
⑤ 系统管理 ^	CPU 使用情况	內存使用情況	
系统设置	CPU 总使用率 1.8%	内存总使用率 60.3% (9.85GB/16.35GB)	
系統信息	I am have the match half	908-	
系统服务	1 ** ~ MMMM WMMMM	698 -	
日志管理	1%-	368 -	
引擎管理	0%	0/08	alua aura
A 用户管理 ~	1702738 1739630 17709780 177171 USAN 1771879 1771879	17.0735 17.08.09 17.08.09 17.11.20 17.12.49	17.16.10 17.15.00
	磁盘使用情况	网络使用情况	
	磁盘 VD 0.00Bps/88.48KBps	同語 1/0 181.17KBps/166.04KBps	
	磁盘使用率 62.0% (75.84GB/122.28GB)		
	🛃 读磁盘 ——	☑ 读网络 ——	
	🖸 万通盘 ——	🛃 写网络 ——	
	160x83pm	BDCKBps]	



4.2.2.1 系统操作

【硬件设备特有功能】 - 系统操作, 可对系统进行操作:

- 重启系统:重启硬件设备
- 关闭系统:关闭硬件设备

4.2.2.2 基本状态

展示系统的整体运行状态和系统运行时长

- 系统运行状态:显示状态正常或者异常或者停止;
- 系统时间:显示系统时间;可以点击更改客户端时间(不建议无端更改,可能会引发未知问题,请谨慎处理)

				1000	-, -, -,	EIRAL	.*±	
系统时间	2022-	-01-0	7 10:	50:58				
	«		20	22年	1月		> >>	
		Ξ	Ξ	四	五	六	日	
	27	28	29	30	31	1	2	取 洞
9周 0天 19	3	4	5	6	7	8	9	
	10	11	12	13	14	15	16	
	17	18	19	20	21	22	23	内存
	24	25	26	27	28	29	30	

■ 若客户端显示的与服务器时间的不符:

服务器时间和您的长亭洞鉴(X-Ray)安全评估系统客户端时间有较大差异,可能导致部分功能异常,请确认客户端所在环境时间是否正常。

- 系统运行时长:显示系统运行时长;
- CPU 使用情况:展示最近 10 分钟的 CPU 总使用率;
- 内存使用情况:展示最近10分钟的内存总使用率、内存总使用量和内存总量;
- 磁盘使用情况:展示最近 10 分钟的磁盘读写情况、磁盘总使用率、磁盘总使用量
 和磁盘总量。



4.2.3 服务状态

在上方分栏中,选择"服务状态",进入服务状态界面。

展示各容器的运行状态,包含容器名称、运行状态、CPU占用率、内存占用率、 运行时长:

、7 响金x	-RAY						admin
认工作区	V	F代目住 / 系统结果					
◎ 全规仪表盘		基本信息 状态监控 服务状态					
13469819	*						
基线管理	<i></i>	容器名称	运行状态	CPU 占用	内存占用	進行时长	
\$ 荒产中心		基线扫描引擎	EW	5	0.07%	6天 23小时 51分钟	
KOTT	×	版本匹配引擎	正常	85	0.59%	6天 23小时 51分钟	
报表中心		任务调度引擎	正常	0.03%	0.29%	6天 23小时 51分钟	
1 man	*	WebSocket 服务面	正常	0.02%	1,05%	6天 23小时 51分钟	
系統管理	10	Web 后白任务	正常	3.03%	30.02%	6天 23小时 51分钟	
系统设置		系统缓存很务	王常	0.12%	D.04%	6天 23小时 51分钟	
系統信息		网页极务器	三米	0.08%	0.07%	6天 23小时 51分钟	
RAWS.		NRIAN	正常	3.05%	1.2696	6天 23小时 51分钟	
引擎管理		数围库服务	正常	0.16%	0.50%	6天 23小时 51分钟	
展の管理	×	关系型数据库连接油	正常	0.12%	0.0395	6天 23小时 51分钟	
		数据仓库服务	正常	7.17%	2.24%	6天 23小时 51分钟	
		Web 应用	шж	0.12%	24.35%	6天 23小时 51分钟	
			X-80	ay XR-810 21.11.001,/10 © 2021 Chame Tech.			

4.3 系统服务

4.3.1 引擎升级

在左侧导航栏中,选择"系统管理-系统服务",默认进入引擎升级界面。


<-> 洞鉴×	-RAY							admin
默认工作区	×	三代甘花 / 系统服务						
◎ 全局仪表盘		引擎升级 漏洞	库升级 备份还)	1 引擎网络诊断 网络诊断工具				
日 約時管理	*							
A 基化管理	<i></i>	当前引擎信息						
5 8 4 40		引擎节点总数 印 擎 节点状态	1 • 工作0 • 空	回1 ● 時間0 ● 野筋(中)0				
* ж лен	- 20	当前演测库版本	6_2021-12-10_r1					
目根表中心		引擎升级						
a man	×	(1) 第一步,选择	要升级的引擎					
系统管理		(FMARRINE)	服以工作区 X	+ 添加器选条件				
原的设置		• 已选择 (115 1					
系统信息			引擎名称	引擎节点	运行状态	可用蜡纸单位	系統版本	最后升级时间
54585			testans	169.254.1.1	空间	顺认工作区	6.0.2 _. r1	2021-12-20 18:15:41
日志管理								
引擎管理		(a) MT-# 184	T1 473 488 494					
「馬や管理	×	M851 21	在线开级	升级历史				
		里斯引擎可!	8号放服务中期, 调	他认所有引擎节点均不处于运行状态,再进行升级操作				
				点击或将交件拖拽到这里上传 上中21等更新在		允许在黑结环境下,就过上代文件的方式 1. 引擎升级仪动引擎节点的能力进行升载 2. 在上方预测中均透射开始的引擎节点 3. 单次仪书记作一个家本程。成击" 4. 状态处于进行中的引擎节点。遗传任美	(进行高线引擎升级。高线升级需要注意 8) 40开级-后,将对上方遗中的引擎节点 58边地后再启动升级。	1以下事项。请仔细阅读说明后进行开始 进行安装更新:

4.3.1.1 内容展示

注: 想要查看所有有权限查看的引擎节点请删掉默认的当前组织单位的筛选条件。 版本信息页面展示当前系统的版本信息,具体包括:

- 引擎节点数
- 引擎节点状态(工作、空闲、异常、更新中的个数)
- 当前漏洞库版本
- 每个引擎节点的版本等相关信息:
 - 引擎名称
 - 引擎节点
 - 运行状态
 - 可用组织单位
 - 系统版本
 - 最后升级时间



벌 10 3 1 31 31 31 31 31 31 31 31 31 31 31 31 31	單值息 學节点总数 學节点状态 前淵淵连版本	1 ● 工作 0 ● 空i 6_2021-12-10_r1	利1 • 异常 0 • 夏斯中 0				
引撃升	级						
0	第一步、选择	要升级的引擎 111111111111111111111111111111111111	+ 浙加湖法条件				
	● 已选择 0	个引擎					
		引擎名称	引撃节点	运行状态	可用组织单位	系统版本	最后升级时间
		testaaa	169.254.1.1	空间	默认工作团	6.0.2_r1	2021-12-20 18:15:41
2	第二步,进行: <mark>高线升级</mark>	升 级操作 在线升级	升级历史				< 1 > 10 船(页>
	更新引擎可能	导致服务中断,调制	14从所有引擎节点均不处于运行状态,再进行升级排	h/T	一键开级		
			点击或将文件拖挽到这里上传 上传引擎更新创		允许在周端环境下、通过上传文件的方式 1. 引擎升级汉对引擎立构的能力进行开级 2. 在上方的每中均选行开始的影響方式 3. 单次仅允许上标一个城本包、点击"一电 4. 状态处于运行中的引擎节点、语待任务/	些行置成引擎升级。面结升级需要注意 " 建升级"后,将对上方选中的引擎节点 信束后再启动升级。	1以下事项,请仔细阅读说明后进行升级: 进行安装更新:

- 系统版本:
 - 系统版本表示洞鉴扫描算法与策略的版本;
 - 系统版本与系统预置的扫描策略、扫描插件等密切相关,更高的引擎版本会有 更优秀的扫描效果;
 - 系统版本可以在版本信息页面上直接更新,详情见下文"引擎节点升级"。
- 引擎状态:
 - 引擎状态表示当前洞鉴的扫描引擎运行状态;
 - 状态有4中类型:
 - ◆ 工作:正在执行扫描任务的节点;
 - 空闲:状态正常且没有执行扫描任务的节点;
 - 异常:状态不正常的节点,这种状态的节点,一般无法正常运行扫描任务,
 异常状态可能存在的问题可以参考当前洞鉴版本的部署文档"常见问题

四"中的解决方法;

◆ 更新中:引擎节点正在进行升级操作时的状态,该状态下不能启动扫描任务。



4.3.1.2 引擎节点升级

在版本升级页面可以直接更新引擎版本。当前支持离线升级和在线升级。

注意:更新引擎可能导致服务中断。若系统有正在运行的任务,则不能更新引擎版本。请停止所有正在运行的任务,再尝试更新引擎版本。

内容展示:显示引擎名称、引擎节点 IP、运行状态、可用组织单位、最后升级时间

操作步骤:更新引擎版本的具体操作步骤如下:

- 确定系统当前的引擎版本、需要的引擎版本,准备对应的引擎更新包;
- 升级模式支持"一键升级全部引擎节点"和"单节点升级";
- 确保系统没有任务处于正在扫描状态。

离线升级:

上传框上传引擎更新包,或将引擎升级包拖拽到此处上传,上传过程显示上传进度

第二步,进行升级操作 <mark>离线升级</mark> 在线升级 升级历史	
更新引擎可能导致服务中断,请确认所有引擎节点均不处于运行状态,再进行升级操作	-w/r.u
	允许在面线环境下,通过上传文件构方式进行面线引擎升级。面线升级重要注意以下事项。请仔细间读说明后进行升级: 1. 引擎开级仪对后擎节点的制力把行开做: 2. 在上方到表中勾动持行级的引擎节点: 3. 单次仪法疗: 这一个效本包。点击一一罐升级*后,将对上方选中的引擎节点进行安装更新:
点击或将文件拖拽到这里上传 上传引家更新回	4. 状态处于运行中的引擎节点。课特任务结束后再启动升级。

● 更新包上传完成后,确认引擎版本是否正确:



- 点击"一键升级";
- 确认引擎版本正确后,点击"确认更新";
- 返回版本信息页面,引擎状态变为"更新中";

■ 引擎更新大概需要十几分钟,期间扫描任务无法正常启动。请耐心等待更新完成。



引擎更新完后,版本信息页面的"引擎版本"相应变化,引擎状态显示"运行正常",则表示引擎版本更新成功

在线升级:

前提:需要注册在线升级平台后方可使用在线升级功能

1. 访问升级服务平台

2. 使用许可证进行注册

3. 点击"更新升级服务平台地址", 输入"https://product-support.chaitin.cn/", 点击"确定"即可

^最 先登录升级服务平台)	进行注册,在线升级功能才可使用,注册步骤:			
.访问升级服务平台				
上传系统使用的 licens	se,进行注册登录			
、更新升级服务平台地均	t.			
1. 升级过程可能会对	正在运行中的扫描任务的扫描结果产生影响,注	升级前请确保没有运行的任务。		
1. 升级过程可能会对 2. 如点击升级后提示	正在运行中的扫描任务的扫描结果产生影响, "无法直接升级该版本",请点击此链接 <mark>获取中</mark>	升级前请确保没有运行的任务。 间升级版本		
1. 升级过程可能会对 2. 如点击升级后提示 版本包名称	正在运行中的扫描任务的扫描结果产生影响,; "无法直接升级该版本",请点击此证接获取中 版本描述	升级前请确保没有运行的任务。 间升级版本 文件大小	版本发布时间	操作
1. 升级过程可能会对 2. 如点击升级后提示 版本包名称	正在运行中的扫描任务的扫描结果产生影响,; "无法直接升级该版本",请点击此短接获取中 版本描述	升级前请确保没有运行的任务。 间升级版本 文件大小	版本发布时间	操作
1. 升级过程可能会对 2. 如点击升级后提示 版本包名称	正在运行中的扫描任务的扫描结果产生影响,; "无法直接升级该版本",请点击此链接获取中 版本描述	升级前请确保没有运行的任务。 间升级版本 文件大小	版本发布时间	操作

● 在第二步选择"在线升级" Tab 后,若有新的可下载的在线升级包,会显示红色气

泡及对应的数量;

- 点击最新引擎版本旁的下载新版本开始下载;
- 下载后可以开始升级。



4.3.2 漏洞库升级

在上方分栏中,选择"漏洞库升级",进入漏洞库升级界面。

- 点击进入系统服务的漏洞库升级中,显示当前漏洞库信息(版本、漏洞总数、上次 更新时间),可通过一键升级或者上传升级包来操作离线升级漏洞库;
- 可以查看升级历史,包含漏洞库版本、漏洞更新描述、开始升级时间、完成升级时间、更新状态。

引擎升级 運興库升級 备份还原 引擎网络诊断 网络诊断工具	
当約還同時信息	
漏回库版本 6_2021-12-10_r1	
包含漏洞总数 165461条 查看漏洞洋情	
上次更新时间 2021-12-03 16:58:59	
漏洞库升级	
高线开绘 在线升级 升级历史	
升级过程可能会对正在运行中的扫描任务的扫描结果产生影响,升级崩溃确保没有运行的任务。	一個升級
	允许在离线环境下,通过上传文件的力式进行面引席更新操作。 有些赢得可能需要同步升级最新引擎版本才可进行检测,如果使用过短发现漏洞库的某些漏泥不支持检测,请接查引擎版本 最否过旧。
点击或将文件拖挽到这里上传 上传属鸡库更新句	

漏洞库升级:

同"引擎升级"中的离线升级和在线升级,且能查看升级历史。

4.3.3 系统升级

展示内容:

- 当前系统版本:
 - 系统版本:显示版本号
 - 上次更新时间:
 - 更新进度:



< ・> 洞瑩 x-яау		admin
数认工作区 ソ	半的装置 / 系统服务	
② 金姆仪表盘	引擎升级 凝洞库升级 系统升级 备份还原 引擎网络诊断 网络诊断工具	
日 扫描管理 · ·	当每系统版本	
小 基础管理 一	系统版本 21.12.001_/2	
5 g/*#0 ~	上次更新时间 2022-01-06 19:15:20	
иния .	更新遗症 更新结束	
◎ 指表中心 ~	系统升级	
⊐ winw ~	黄婧升级 升级历史	
D 系统管理 ^	更新系统可能导致服务中新,请确认当的没有紧急需要执行的任务,再进行升级操作	一城)中間
系统设置		化并在集越环境下。通过上传文件的方式进行集线系统开级。属线开始需要注意以下事项。语行组成读说将后进行 开始: 1. 氟硅升级等均量个系统进行升级:
系統服务	点击或将文件拖拽到这里上传	2. 电次仪冗许上述一个版本包。点击"一般开始"面。将对当时多高度本进行开始到上述包中的目标系更能不 3. 系统升级不可与其他引擎升级或测成升级同时进行。否则会出现异常
日志解釋	上传系就更新包,文件大小不超过4G	
引擎管理	X Pay XP-	510 21.12.001 / 2 / 0 2521 Charlon Tech.
▲ 用户管理 ~		

系统升级:

- 离线升级:可以通过上传升级包(小于 4GB)后一键升级。升级过程中任务会中断, 且不能与引擎同时升级。
- 升级历史:可以查看历史升级的相关情况。

4.3.4 备份还原

<・> 洞罂x	RAY			admin
默认工作区	×	平式甘语 / 系统服务		
◎ 全局仪表盘		引擎升级 漏洞库升级 备份进展 引擎网络诊断 网络诊断工具		
日相相推	*	ANNERSTINGS (AND DEPENDE STREET AND		
A 基线管理	<i>.</i>	 Research and the second se second second sec		
5 <u>R</u> ^++0		备份列表		截然备份设置 收起
⇒ KREH	$^{\otimes}$	创建备金点		
自 报表中心		ADVA ADVA	8.00H0	Terc+ 48
a wan	×	■ 17.4/mm ■ 17.2/m/	III LUMUM	JAMET BUT
② 系积管理	10			
累积投票		能无效加		
系统信息				
545A				4 1 5 10条/页~
日志管理				Particul Parameter Statement (Statement)
引擎管理		还顺历史		10.20 10.20
る 馬を管理	×	上版文档法编		
			10 M M + 10 Jr	-
		北線電気信件	达粮至时间点	SWETHER METERS
		10元四日		

备份还原提供备份系统数据库、还原系统数据的功能。



4.3.3.1 系统备份

备份数据包括扫描任务,任务结果、资产数据信息、漏洞数据信息、日志审计信息 等。备份时需预留磁盘容量,避免恢复后出现数据丢失。

此处以备份列表展示备份记录。

			数据备份设置 收退	a la
	备份时间	系統版本	操作	
<u>〔11</u>] 首天政語				
			< 1 > 10.条/页∨	
	N K K H	8 0 00 	後分时间 X/()版本 () () ()	数据数分加速 0.3 金分时间 系統版本 操作

- 点击列表上方"创建备份点",可编辑备份名称,点击确定后开始备份;备份期间请 勿离开当前页面,否则会取消当前备份任务;
- 可在【系统设置】--【基本配置】中开启自动备份功能,详见<u>4.1.1.5数据备份配置;</u>
- 开始创建备份点后,备份列表会出现一条新记录,展示备份状态、备份名称、备份
 时间、系统版本和可进行的操作;
- 待备份完成后,可对备份点进行备份文件下载至本地、在线还原、删除操作:
 - 点击在线还原,可将系统还原至该备份点,当前系统数据被覆盖。



4.3.3.2 系统还原

可通过备份列表,对某备份点在线还原,或者上传备份文件手动还原,可还原历史 版本和当前版本的备份文件。系统还原列表记录还原操作历史。

 点击列表上方的"上传文件还原",选择本地的备份文件,上传结束后,会解析 出备份文件相关信息,点击"确认恢复",将对备份数据进行还原

还原历史				100	nu:
上传文件还积					
还原备份名称		还原至时间点	操作用户	操作时间	
	加无权派				

4.3.5 引擎网络诊断

在上方分栏中,选择"引擎网络诊断",进入引擎网络诊断界面。

用于诊断每个扫描与扫描目标的连通性,用于测试引擎节点与目标 IP 之间的连通性,具备 ping、traceroute 和 nmap 命令进行网络诊断:

<・>洞鉴x	-RAY			admin
默认工作区	V	系统管理 / 系统服务		
② 全局仪表盘		引擎升级 漏洞库升级 系统升级 备份还顾 弓	掌网络诊断 扩展管理平台配置	
□ 扫描管理	×	用于诊断偏个引擎与扫描目标的连通性		
8 基线管理	~			
◎ 遼产中心	~	引擎节点	引擎节点:10.9.33.33	
△ 藻洞管理	*	• 10.9.33.33	ping traceroute namp	
窗 报表中心	×	• 100.244.1.143	请输入 mmap 的 IPv4 / 域名 地址 namp	
🖸 知识规	*	 100.244.1.144 10.9.33.186 		
◎ 系統管理	^	• 10.9.33.182	····································	
系统设置			nmap 输出结果	结束运行
系统信息			None core report for baraling wil at (18 2 8 5)	
系统服务	1		Host is up (0.0071s latency).	
日志管理			PORT STATE SERVICE VERSION 22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)	
引擎管理			Service Info: 05: Linux; CPE: cpe:/o:linux:linux_kernel	
△ 用户管理	×		Service detection performed. Please report any incorrect results at https://nmap.org/submit. # Nmap done at Fri Apr 14 10:47:55 2023 — 1 IP address (1 host up) scanned in 0.51 seconds	/ .

● 选择命令: ping、traceroute 或 nmap;



● 填入目标 IPv4 或者 IPv6 地址,点击按钮进行连通性测试,后查看结果。

4.3.6 扩展管理平台配置

系统管理 / 系统服务		
引擎升级 漏洞库升级 系统升级 备份还原 引擎网络诊断	扩展管理平台配置	
当前扩展管理平台信息		
平台版本 -		
启用情况 未启用		
安装配置时间 -		
扩展管理平台配置		
1 第一步,请下载扩展管理平台配置文件 获取配置文件		
2 第二步,获取安装包后根据配置文件部署扩展管理平台,部署过	程请联系技术支持	
3 第三步,从扩展平台获取所需参数填入并启用扩展平台		
配置扩展管理平台后,用户管理将在平台中进行,长亭洞鉴(X-Ray)	安全扫描系统仅将含用户角色权限及组织单位的管理功能	
扩展平台启用配置	sata 🕥	
client_ID -		
系统地址 -		
扩展平台地址 -		

可查看当前扩展管理平台的配置信息,还可以通过三步完成对扩展平台的配置。



4.4 日志管理

4.4.1 操作日志列表

<・> 洞鉴x-	RAY					admin
默认工作区	V F	-CTT / B&MT				
◎ 金属仪表盘			× + 添加筛选条件			
日白柳樹地	*	已选择 0 个操作日志		专主法中的日志		
A 最优级地	<i>.</i>	口 用户名	IP	管理员角色	操作日志描述	操作时间
書 資产中心	~	admin		1010-06102-03	atron 否如的目標任果ELV告诉在世了目標任果ELE:「2021.19.07 17:57-26】 LLVEI期提表	2021-12-27 17-28-42
☆ 実行管理	- 20	autorities and a second		899.999 (B) (B) (4)	warms with a state of the state	and the set of an area
山 根表中心		admin	10.2.4.210	組織管理目	admin 跟加了扫描任务 IlurY	2021-12-27 17:37:26
13 man	*	admin	10.2.4.210	超線管理员	admin 整要成功,验证方式: 密码	2021-12-27 17:37:25
© 8488	ं	admin	10.2.4.210	超级破坏员	admin 健豪成功,检证方式: 撤销	2021-12-27 17:37:24
原航设置		admin	10.2.4.195	超级管理员	admin 雅雯成功,暗证方式: 密码	2021-12-27 17:09:44
系统信息		admin	10.2.5.169	超级管理员	admin 登录成功,验证方式: 密码	2021-12-27 17:01:38
##BB		C] admin		超级管理员	admin 返加的扫描任务SoRM(自动生成了扫描任务报表: 【2021-12-27_16-46:57】SoRM(扫描报题	2021-12-27 16:48:21
日本業成		admin	10.2.4.210	組織領導品	admin 派加了扫描任务 ScRMJ	2021-12-27 16:46:57
引擎管理		admin	10.2.4.210	超级管理员	admin 登录成功,独远方式: 密码	2021-12-27 16:46:56
◎ 局户管理	×	admin	10.2.4.210	超级管理员	admin 發發成功,續這方式: 准码	2021-12-27 16:46:56
					< 1 2 3 4 8 ···· (137 >	10条/页> 跳至 页
					x-Neg x01-510 21.11.001_r10 80.0011 Chasten Texn.	

4.4.1.1 内容展示

主要展示使用洞鉴的所有用户的操作日志,内容包括用户名、IP、管理员角色、操 作描述、操作时间:

0 8	选择 0 个操作]	日志 图称选中的操作日志	尊出遗中的日志		
	用户名	Ib	管理员角色	操作日志描述	操作时间
	admin		超级管理员	admin 添加的扫描任务iluv自动生成了扫描任务报表: 【2021-12-27_17-37-26】 liuv扫描报表	2021-12-27 17:38:4
	admin	10.2.4.210	超级管理员	admin 添加了扫描任务 IJuY	2021-12-27 17:37:2
	admin	10.2.4.210	超級管理员	admin 登录成功,检证方式: 密码	2021-12-27 17:37:2
	admin	10.2.4,210	超级管理员	admin 登录成功,验证方式: 密码	2021-12-27 17:37:2
	admin	10.2.4,195	超级管理员	admin 登录成功,验证方式: 密码	2021-12-27 17:00;4
	admin	10.2.5.169	超级管理员	admin 整录成功,检证方式: 密码	2021-12-27 17:01:3
	admin		粗级管理员	admin 添加的扫描任务ScRM;自动生成了扫描任务报表: [2021-12-27_16-48:57] ScRM;扫描报表	2021-12-27 16:48:2
	admin	10.2.4.210	超級管理员	admin 添加了扫描任务 ScRMJ	2021-12-27 16:46:5
	admin	10.2.4.210	超級管理员	admin 登录成功,验证方式: 密码	2021-12-27 16:48:5
	admin	10.2.4.210	超级管理员	admin 登录成功,验证方式: 密码	2021-12-27 16:48:5

4.4.1.2 添加筛选条件

- 点击添加筛选条件,从用户名、管理员角色、操作关键词、操作时间、所属组织单位;
- 可以采用精确匹配或者模糊匹配的方式;
- 点击保存生效;
- 可以在弹窗或者列表中删除已经设定的筛选条件。

0 ES	目径 1 个操作日志	删除选中的操作日志	导出选中的日志		
×.	用户名	IP	管理员角色	操作日志描述	操作时间
	admin		超级管理员	admin 添加的扫描任务II(uY自动生成了扫描任务报表: 【2021-12-27_17:37:26】II(uY扫描报表	2021-12-27 17:38:42
	admin	10.2.4.210	超级管理员	admin 添加了扫描任务 IijuY	2021-12-27 17:37:26
	admin	10.2.4.210	超级管理员	admin 登录成功,输证方式: 密码	2021-12-27 17:37:25
	admin	10.2.4,210	超级管理员	admin 登录成功,检证方式: 密码	2021-12-27 17:37:24
	admin	10.2.4,195	超级管理员	admin 登录成功,验证方式: 密码	2021-12-27 17:09:44
	admin	10.2.5.169	超级管理员	admin 整录成功,输证方式: 密码	2021-12-27 17:01:38
	admin		超级管理员	admin 添加的扫描任务ScRM自动生成了扫描任务报表: 【2021-12-27_16-46:57】 ScRM 扫描报表	2021-12-27 16:48:21
	admin	10.2.4.210	超级管理员	admin 微加了扫描任务 ScRMJ	2021-12-27 16:46:57
	admin	10.2.4.210	超级管理员	admin 登录成功,验证方式: 密码	2021-12-27 16:46:56
	admin	10.2.4.210	超级管理员	admin 登录成功,检证方式: 密码	2021-12-27 16:46:56

用户名	×	请输入要筛选的内容	模糊匹配>	
+ 添加筛选条	件			

4.4.1.2 批量操作日志

只有有日志管理权限的人才可以批量导出和删除日志。

 选择要导出/删除的日志,然后点击"导出/删除",即可自定导出并下载 json 文件或 删除日志。

						长亭神
18.7	日志管理					
Make	R#G 默认工作	tistofiis + stofiis	条件			
o ei	書種 10 个操作	日志				社動操作
	用户名	IP	管理员角色	操作日志描述	10	(FFF) (平出)
2	admin	10.6.6.199	超级管理员	admin 登录成功,检证方式:Oauth	20	23-07-12 11:15:
2	admin	10.10.5.199	超级管理员	admin 登录成功,验证方式:Oauth	20	23-07-12 11:12
2	admin	10.6.8.230	超级管理员	admin 登录成功,验证方式: Oauth	20	23-07-12 10:30
1	admin	10.6.6.230	超级管理员	admin 登录成功,验证方式:Oauth	20	23-07-11 17:05
2	admin	10.6.5.102	超级管理员	admin 生成了基核检查报表: 基线142	20	23-07-11 16:27
2	admin	10.6.5.102	起级管理员	admin 登录成功,检证方式: Oauth	20	23-07-11 16:23
2	admin	10.6.5.217	超级管理员	admin 修改了任务 1	30	23-07-11 15:42
2	admin	10.6.5.217	超级管理员	admin 添加了扫描任务 2	20	23-07-11 15:42
2	admin	10.6.5.217	超级管理员	admin 修改了任务 1	20	23-07-11 15:41
2	admin	10.6.5.217	超级管理员	admin 添加了扫描任务 1	20	23-07-11 15:41:
					< 1 2 3 4 5 40 > 10象/页	林至

4.5 引擎管理

注:洞鉴在第一次使用时,引擎列表内无引擎节点,需要将筛选项"默认工作区"删 除后,方可看到所有引擎,然后点击编辑,将之分配到"默认工作区"或目标工作区后继 续使用。

4.5.1 引擎列表

在左侧导航栏中,选择"系统管理--引擎管理",默认进入引擎列表界面。

			112					
扫描管理	~	0 已选择 0	个引擎 图称适中的	NI章 配置统一 DNS				
基线管理	*		刘敏在卧	2184410	104040	2180 4000	45.90	18.0
资产中心	~		り事合称	刘章卫团 16	18114/18	51年代/8	10.22	SHIF
展测整理	~			169.254.1.1	 空闲 	自定义权限	*	宣看 编辑 删除
报告管理	*							< 1 > 10条/页
知识库	~							
系统管理	^			did-m	ww-511 21.04.001_+6 @ 2021	iddddf Tech.		
系統设置								
系统信息								
系统服务								
日志管理								
日志管理								



4.5.1.1 内容展示

在引擎管理页面中,以列表方式展示所有引擎节点的相关信息,包括引擎名称、引擎节点 IP、运行状态、引擎权限、标签、CPU 总使用率和内存总使用率、以及对应操 作选项。

引擎列表 其他扫描	配置							
所属组织单位 默认工作器	[×] + 添加筛选条件							
 已选择 0 个引擎 	●部本中的引擎 图面积一 DNS							
□ ✓ 引筆名称	引擎节点 IP	运行状态 弓	引擎权限	柳篮	CPU 总使用率	内存总使用率	运行时长	操作
🗍 testaaa	169.254.1.1	 空闲 	自定文权限	11	2.2%	92.7% (15.15GB/16.35GB)	7周 4天 2小时 24分钟	28 SH ER
								〕 〕 10 祭/預∨

4.5.1.2 筛选操作

点击列表上方"添加筛选条件",可根据引擎名称、引擎节点 IP、运行状态、所属组 织单位对列表中的引擎进行筛选。

nimmin / 518	PHERE									
引筆判表	网络白杨伦里									
十 透加羽	送条件							0.000		
0 E31	0 个引擎							自动術新 🛈 🤇	00	批量操作 ~
	引擎名称	引擎节点 IP	运行状态	引擎权限	标签	CPU 总使用率	内存总使用率	运行时长	操作	
	e.	169.254,1.1	• 空闲	公有		2.1%	59.9% (9.63GB/16.08GB)	4周2天1小时17分钟		ieur Bur
									1 >	10 张/页

4.5.1.3 批量操作

व्याप्राय / हा	南 県道									
518918	A GREEK									
+ 38.00	筛选条件									
 已満 	择1个引擎								00	肥業操作、イ
2 -	引筆名称	引擎节点 IP	运行状态	引擎权限	标签	CPU 总使用率	内存总使用率	通行时长	操作	删除 配置 DNS
	20	169.254.1.1	• 空闲	公有	1.00	1.9%	60.2% (9.68GB/16.08GB)	4周 2天 1小町 22分钟		58.18 B19
									1	10 象/页 ~

删除引擎

勾选选择一个或多个引擎后,可点击"批量操作"-"删除",对引擎进行删除:

● 若选中删除的引擎包含内置引擎,则无法删除;

若删除的引擎有关联的扫描任务,则系统会返回相关任务列表,需在扫描任务的配置中修改引擎选择后,重试删除操作,才可成功删除。

配置统一 DNS

● 点击列表"批量操作--配置 DNS",参考 4.5.2.2 域名解析配置

4.5.1.4 查看引擎详情

基本信息 引擎名称 testaaa 运行状态 空间 169.254.1.1 运行时候 7周 4天 2小时 31分钟 引擎节点中 版本号 标签 6.0.2_r1 版本升级 自定义权限 引擎权限 最后升级时间 2021-12-20 18:15:41 高级配置信息 肉起 被动影虫服务器配置 城名解析配置 基于代理的被动原虫的代理服务器配置 DNS 服务器 10.3.0.1 静态 host 配置 代理服务器 IP 10.2.19.1 盲打平台配置 HTTPS 根证书 ② 点击下载 HTTPS 根证书 盲打平台名称 內實實打平台 查看盲打平台详情 基于日志的被动愿虫的 Syslog 最务概配算 Syslog 服务器 IP 169.254.1.1 实时状态 CPU 使用情况 内存使用情况

点击操作列的"查看",可以查看节点详情:

基本信息

展示引擎节点名称、引擎节点 IP、标签、引擎权限、引擎运行状态、运行时长、引 擎版本号、最后升级时间

 点击版本号右侧的"版本升级"按钮,可跳转至【系统服务】--【引擎升级】页面进 一步操作;

高级配置信息

展示该引擎节点的被动爬虫服务器配置、域名解析配置信息;

实时状态



该引擎节点的 CPU 状态、内存状态、网络状态、磁盘状态,与上文介绍的【系统 信息】--【状态监控】数据指标一样

4.5.1.5 编辑引擎

点击操作列的"编辑",可以编辑引擎节点的信息:

编辑引擎		×
引擎基本信息		
引擎节点 1	00.244.1.144	
引擎名称	请输入引擎名称对引擎进行描述	
* 引擎权限	自定义权限	\sim
* 组织单位	₩HYL-₩HYL02 × ₩HYL × HYL	0
标签	₩HYL-23.02.001-白名单v3-白 HYL-23.02.001-白名单v3-白子B-后加组织单位-谁删 ₩HYL-23.02.001-白名单v3-白子B-后加组织单位-谁删	
盲打平台监听配置 为存储型 XSS、SSRF = 本系统服务器的 IP 地址	₩HYL-23.03.001-99/2019 ####100 WHYL-23.03.001-时间窗 WHYL-23.03.001-扫描深度_自定义	
*选择盲打平台	₩HYL-23.03.001 ₩HYL-全量_gunkit	
被动爬虫服务器配置	₩HYL-23.02.001-白名单v3-白子B-后加组织单位 发起	
基于代理的被动爬虫的代	代理服务器配置	
以下代理服务器,用于为	b被动 Web 漏洞扫描任务提供需要的代理服务器信息。	
代理服务器 IP	100.244.1.144	
HTTPS 根证书 ⑦ ,	点击下载 HTTPS 根证书	
	取消	确定

引擎基本信息

可编辑引擎名称、权限、组织单位等属性,组织单位针对工作区全程支持模糊匹配功能。

被动爬虫服务器配置

配置该引擎节点的被动爬虫服务器,与4.5.2.1 被动爬虫服务器配置实现相同功能。

域名解析配置



与 4.5.2.2 域名解析配置实现相同功能。

4.5.2 其他扫描配置

<→洞鉴x	-RAY		admin	
默认工作区	V	不成於位 / 引擎管理		
◇ 全局仪表盘		引擎对表 其他白细胞度		
日白板管理	٠			
A 基线管理		被动都中服务器配置	88	
★ 資产中心	×			
☆ 展行管理	$^{\otimes}$	引擎节点	引擎节点 160.254.1.1	
自 相表中心		• 169.254.1.1	基于代理的海边爬出的代理服务类配置	
	×		以下代增服务绩,用于为被没 Vaio 赢得已接任务是负需要的代电服务器信息。就以减口范围可以避免防火地等网络配置对服务端口的指制,不填表示无限 如 元年年年时期至于时口宫即 时年月期间在各部	
◎ 系統管理	1		10.01139年9日により通知時間に、10.01012月1日日間には、 平静能を見ば 10.2191 /	
系统设置				
系统信息			使地 HTTP TC增加可能按数的物格产面使用 HTTP5 的MCE。下值 HTTP5 相址 节开发 推可解决因问题。	
系统服务				
日志敏速			基于日本的推动增生的 Syndog 服务提定費	
19999			winn (mynowy manyowa), min 1 20mm 1 La varanteka (winn annen Lanin 2 20mm manyo ka ka zo ka ka za ka zo ka ka z Si valon 解表剤 P 160 254 1 1 /	
态 展华管理	×			
		域名解析配置	26	

4.5.2.1 被动爬虫服务器配置

在使用被动 Web 扫描(代理) 和被动 Web 扫描(日志) 这两个被动扫描策略时, 需要在此处进行配置操作。

代理服务器 IP 和 Syslog 服务器 IP 默认为各节点的服务器 IP,用户可以在这里 查看、配置、修改代理服务器的 IP 和端口范围。

每个节点单独配置,不支持统一配置。

被动爬虫服务器配置	88
引擎节点	引擎节点 109.254.1.1
• 169.254.1.1	基于代理的被动爬虫的代理服务器配置
	以下代理服务器,用于为被因 Web 讓同日攝任务提供農業的代理服务器信息,繁认成口范面可以直免的火墙制网络配置对服务端口的限制,不堪表示无限 制。若任务争独配置了端口范围,则优先使用任务配置。
	代理服务器 IP 10.2.19.1 🧾
	使用 HTTP 代現后可能合影响整户编使用 HTTPS 的网站,下载 HTTPS 假证书并安装可解决该问题。
	HTTPS 根证书 点击下载 HTTPS 根证书
	基于日志的被动爬虫的 Syslog 服务错配置
	以下 Sysiog 服务键,用于为基于日志的被动 Web 赢得扫描任务提供需要的代理服务器信息。
	Systog 服务器 IP 169.254.1.1 🖉



基于代理的被动爬虫代理服务器配置

此处配置用于该引擎节点可运行被动 Web 扫描(代理)任务。

- 代理服务器 IP: 默认为引擎节点 IP, 点击"编辑"图标可手动修改;
- HTTPS 根证书:使用 HTTP 代理后可能会影响客户端使用 HTTPS 的网站,下 载 HTTPS 根证书并安装可解决该问题。

基于日志的被动爬虫的 Syslog 服务器配置

此配置用于被动 Web 漏洞扫描(日志)这个扫描策略,用于为该扫描策略提供需要的代理服务器信息,收集日志中的相关信息。

● Syslog 服务器 IP: 默认为引擎节点 IP, 点击"编辑"图标可手动修改。

4.5.2.2 域名解析配置

如果用户希望在扫描主机资产时,使用自定义的 DNS 服务器、或自定义的静态 host 配置来解析域名,可以在此处配置相应信息。

所有节点可以统一配置 DNS 服务器或每个节点单独配置服务器:

统一配置 DNS 服务器:

● 点击"统一配置 DNS 服务器", 弹框如下图所示:



DNS 服务器	1.1.1.1 2.2.2.2	
静态 host 配置	1.1.1.1 test.com 2.2.2.2 test.test1.com	,
选择引擎节点	169.254.1.1 ×	

- 填写 DNS 服务器信息:
 - 如果配置了 DNS 服务器,当洞鉴的一个主机扫描任务尝试解析域名目标时, 将依次向已配置的 DNS 服务器发送 DNS 请求。
 - 在输入框内输入 DNS 服务器的 IP 地址,可同时输入多个 IP, 以换行分隔。
- 填写静态 host 配置信息:
 - 如果配置了静态 host,当洞鉴的一个主机扫描任务尝试解析域名目标时,将 首先尝试用此处配置的静态 host 来解析;
 - 在输入框内配置静态 host, 可同时输入多个静态 host 配置, 以换行分隔。
- 选择引擎节点:
 - 默认选中全部引擎节点,可自由定义要应用的引擎节点。
- 点击"确定",即完成配置。



域名解析配置			45.3
5]攀节点	统一配置 DNS 服务器 引擎节点 169.254.1.1		
• 169.254.1.1	配置 DNS 服务得。	用来解析扫描时遇到的域名	
	DNS 服务器	10.3.0.1 10.3.0.1	
	靜态 host 配量	1.1.1.1 lest.com 2.2.2.2 test.test1.com	

单节点配置 DNS 服务器:

在每个节点右侧显示的 DNS 服务器和静态 host 配置处, 修改相应信息即可。配置方案如下:

- DNS 服务器:
 - 在输入框内输入 DNS 服务器的 IP 地址,可同时输入多个 IP, 以换行分隔;
 - 点击"保存",即完成配置。
- 静态 host 配置:
 - 在输入框内配置静态 host, 可同时输入多个静态 host 配置, 以换行分隔;
 - ◆ 静态 host 的格式为: 主机 IP 地址 + 域名, IP 和域名间至少要有一个 空格。
 - 点击"保存",即完成配置。

五、用户管理

此模块主要用于企业对使用洞鉴的用户的管理,包括添加用户、删除用户、修改 用户信息,查看操作日志等。

5.1 系统用户管理

5.1.1 系统用户管理

在左侧导航栏中,选择"用户管理-系统用户管理",进入系统用户管理界面。

<・> 洞鉴×	-RAY							admin
默认工作区	V I	1/11年 / 系统用户管	理					
◎ 全规仪表盘		HARDSHE MA	工作区 ×	+ 浙加锦选条件				
日白板管理	*	已选择 0 个用	P	Set-strong in the second se				+ 孤雄一个用户
J 基线管理	<i></i>		10 ID	用户名	RCSS	RACE	有效日期至	19/1
营资产中心			51/5) 	100 10				
☆ 展示管理	*	10. 1		admin	最近300 WE FEE CO	.*	1	4214 (2.4)
自 报表中心								< 1 ≥ 10 乗/褒∨
I wan						3-Ray XR-510.21 11:001 /10 0 2021 Charten Nech.		
◎ 系統管理								
二 周戶管理	0							
系统用户管理	J							
用产角色设置								
盤祭拳位筆種								

5.1.1.1 内容展示

系统用户管理页主要展示使用洞鉴的所有用户的信息,内容包括用户 ID、用户名、 用户角、联系邮箱和有效日期等:

● admin 为洞鉴部署时的默认用户,用户 ID 为1,用户角色为系统管理员;

 ////////////////////////////////////	@ 默认工作区 ×	+ 添加释遗条件				+ 透如一个用户
	用户ID	用户名	用户角色	联系劇箱	有效日期至	操作
	1	admin	組級管理员	2	21	1112 D.0
						< 1 > 10条/页√



5.1.1.2 筛选操作

可以通过用户名称、用户角色及所属组织单位对列表中的用户进行筛选。

5.1.1.3 添加用户信息

● 在系统用户管理页面可以添加用户,

 ・用户名 ・密码 ・密码 ・磁认密码 取系电话 取系电话 (取系电话 (取系电话 (取系电话 * 所属组织单位 ① haha) 默认工作区 * 用户和@ 系统管理员 相户权限 教ェ統计 全局仪表盘 任务管理 (正务定法 	添加一个用户		
 密码 - 确认密码 - 确认密码 取系电话 取系电话 - 所属组织单位 ① _ haha - 数以工作区 * 用户角色 系统管理员 用户权限 - 数据统计 全局仪表量 任务管理 任务管理 任务管理 研加和编辑 周路 - 任务信息 任务信息 任务信息 任务信息 百方名 	* 用户名		
 ・ 确认密码 	*密码		
	* 确认密码		
	联系电话		
* 所屬銀织单位 ②	联系邮箱		
* 用户角色 系統管理员 用户权限 - 数据统计 全局仪表盘 - 任务管理 任务统计 - 任务策略 添加阳编辑 删除 - 任务信息 任务下发 副除	* 所属组织单位 ①	 □ haha > □ 默认工作区 	
用户权限 - 数据统计 全局仪表盘 - 任务管理 任务统计 - 任务策略 添加和编辑 删除 - 任务信息 任务下发 副除	* 用户角色	系统管理员	
副院	用户权限	 数据统计 全局仪表盘 任务管理 任务航计 任务策略 添加和编辑 删除 任务信息 任务下发 	
		aite	

5.1.1.4 修改用户信息

● 在系统用户管理页面可以编辑现有的用户

日选择	0 个用户 #11	8进中的用产				+ 添加一个用
	用户ID	用户名	用户角色	联系創稿	有效日期至	操作
	Ť	admin	超級懷理然	ă.	2	5818 SP 82
						< 1 > 10 泰/页

- 在弹窗中根据文案提示,填写修改后的密码、确认密码:
 - 若不填写密码,则表示不修改旧密码。



女用户信息		×
* 管理员角色③	超级管理员	×.]
用户名	admin	
* 密码	为空表示不停改旧密码	
* 确认密码		
用户权限	 数据统计 全局仪表盘 任务管理 任务统计 任务策略 添加和编辑 删除 任务信息 任务信息 任务下发 删除 打描配置 	
	 添加和编辑 删除 报表管理 报表信息 生成报表 	

5.1.1.5 批量操作

在系统用户管理页面可以批量删除和导出用户信息。

FOLLIER AND	1 请不要删除测试	赵将战派 + (× 围8	谢件				
已遗择	9 介用户						11.単純字 ~ 14.00~个用
•	用户ID	用户名	用户角色	联系邮箱	用户状态	有效日期至	田時 特出
	1	admin	题级管理员	*	鹿用	-	1411 215
	2	tht	系统管理员	5 1	启用	#C	
	з	hyl01	系统管理员		应用		
•	4	hyi02	系统管理员	đ	尼用	*	
	5	hyi03	系统管理员	4	启用	27	
-	7	ýdý	系统管理员	÷	此用		
-	10	xiaoming	系统管理员	*	此用	*	
	12	chanpin02	系统管理员	4	启用	2	
8	20	hid	系统管理员		启用		M50 2-8 819
	23	Ih02	系统管理员		启用		

5.2 用户角色设置

主要定义登录系统的管理员角色,不同的角色可以设置不同的管理权限,只有安全 保密管理员才可以对系统角色进行管理。

5.2.1 用户角色列表

在左侧导航栏中,选择"用户管理-用户角色设置",进入用户角色设置界面。

<->洞₩×-	RAY					admin
从工作区	V. P	2个时间 / 用户角色设置				
○ 全局仪表盘		如田田市市在 繁认工作区 ×) + 酒加等选条件				
1040404	*	 已选择 0 个角色 100 送日 0 个角色 				+ 調加一个角色
《 基线管理	аў.	□ 角色名称	角色描述	创建单位	角色漆加日期	細作
\$ 荒产中心	×	□ 系统管理员	可对系统业务功能和系统用户进行管理	系统创建	2021-11-25 10:48:34	26
展示管理	*	的人们讲解读者	1747年1月1日日本440月1日1日日 日本1751年月1日本4日本1日本	WALLOW		
根表中心		文工体出展境内	可对永武管理员的用色仅被进行管理,同时可以发展看永式用户管操作日志	來可從國	2021-11-25 10:46:34	近 報
1 man	\approx		可重着系统用户的操作日志,对系统的所有用户行为进行监督	系统创建	2021-11-25 10:48:34	登積
系统管理		□ 超级管理员	可对系统业务功能。系统用户和操作日本进行管理	苏机能建	2021-11-25 10:48:34	20
局戶管理	10	福作日志管理员	可管理系统用户的操作日志,对系统的所有用户行为进行监督	系统创建	2021-11-25 10:48:34	
系统用户管理					1	10 泉/百一
用产角色设置						
组织单位管理			X-Ray 30-8102111.201,y10 0.2021 Chaste Tach.			

5.2.1.1 内容展示

显示角色名称、角色描述、创建单位、角色添加日期。

- 其中系统管理员、安全保密管理员、操作日志审计员、超级管理员、操作日志管理员系统管理员、安全审计员是系统内置的管理员角色,不可被更改或删除。
 - 超级管理员:只包含一个 admin 账户,不可设置其他账户,不允许被删除,该 账号只对其自己可见。可以增删改查系统用户和角色,可以查看导出删除日志, 查看修改系统信息;
 - 系统管理员:管理操作系统业务功能,对系统用户进行管理。可以查看系统用 户和角色,可以查看系统信息;
 - 安全保密管理员:对管理员角色进行管理,增删查改系统角色,对系统操作日 志进行审查;
 - 操作日志审计员:查看系统用户操作日志;
 - 操作日志管理员:查看、导出、删除系统用户操作日志。



n m	пох 请不要删除测试数据 × + 添加除选条件						
BI	选择 0 个角色			虹屋操作 シ	+ \$	86	M
	角色名称	neau	创建单位	角色道加日期	操作		
	系统管理员	可对系统业务功能和系统用户进行管理	Kittitil	2022-12-14 15:18:33	-		
	安全保密管理员	可对系统管理员的角色权刚进行管理,同时可以直着系统用户的操作日志	系统创建	2022-12-14 15:18:33			
	操作日志审计员	问邀着某他用户的操作目录。对某他的听我用户行为进行监督	系统创建	2022-12-14 15:18:33	2.6		
	操作日志管理员	可管理系统用户的操作日本,刘系统的所有用户行为进行监督	原机能調	2022-12-14 15:18:33	121		
	空权服务色	用户自动初始化隽色,无权删	系統包建	2022-12-14 15:18:36	21		
	пемтоїе		请不要删除测试数据	2023-06-09 17:42:46	5636	2.W	
	test	123	请不要删除测试数据	2023-06-30 14:18:03	5531	位有	
	仪任务管理		请不要删除测试数据	2023-05-30 17:59:23	18.91	21	8
	自定义角色产品test		请不要删除测试数据	2023-07-04 16:28:20	618	24	

5.2.1.2 筛选用户角色

点击列表上方"添加筛选条件",可根据角色名称,角色使用单位进行筛选。

和筛选条件			
角色名称	V	请输入要筛选的内容	
+ 添加筛选条件			

5.2.1.3 添加自定义管理员角色

安全保密管理员可以按需增加系统管理员角色,并赋予管理员角色权限

- 点击"添加一个角色"按钮,按照弹框提示一步步操作即可,分别填写相应内容
 基本信息:
 - 角色名称: 定义角色的名字,供管理员创建用户时选择;
 - 角色描述:对定义的管理员角色,进行简要说明。
- 操作权限设置:
 - 业务功能管理:可对系统的所有业务功能进行查看、操作、管理;
 - 用户管理: 可对登录系统的用户进行管理。
- 访问权限设置(IP 白名单):



- 这里可以对允许角色登录的 IP 进行设置;
- 不设置默认不做任何限制;
- 填写了 IP 后,该角色只能在设置的 IP 下可以登录。
- 信息确认:

■ 查看前面填写的角色相关信息,确认无误时,点击"完成"即可成功创建角色。

角色基本信息							
	. <i>16.4</i> .47.17	100 M 1 44 44 44 44 14					
	* 角色名称	1-32 个不如含原格的字符					
	角色描述	请输入角色描述。便于使	建建入面色描述 停于使用者回到波面色				
	num.	In any variation no. Inc. A mouth news rate					
	*角色创建单位 ①	默认工作区					
	IP白名单	CED					
角色功能权限							
功能模块		功能模块显示控制	操作权跟控制				
□ 数据统计		全局仪表盘					
任务管理		任务统计					
		任务策略	(Ribbi RD (Q + II)	□ 動除			
		任务信息	□ 任务下发				
		扫描配置	调整为1400%和1				
□ 报表管理		报表信息	□ 生成报表				
		报表模板	□ 滚加和编辑	- BIR			
资产管理		资产全景					
		资产信息)液动和3%和				
		资产属性		- BIR			

5.2.1.4 删除管理员角色

可以对自定义的管理员角色进行删除。

角色结	用#© 请不要删除别试数据 × + 须加落选条件							
0 E	选择 4 个角色			F	出现终行 ~	+ 8	iho—	A 1
	角色名称	角色描述	创建单位	#Bi	BIR	操作		
	系统管理员	可对系统业务功能和系统用户进行管理	系統创建	2022-12	-14 15:18:33	28		
	安全保密管理员	可对系统管理员的角色权限进行管理。同时可以查看系统用户的操作日志	系統创建	2022-12	-14 15:18:33			
	操作日志率计员	可查看系统用户的操作日志,对系统的所有用户行为进行监督	系统创建	2022-12	14 15:18:33	21		
	操作日志管理员	可管理系统用户的操作日志,对系统的所有用户行为进行监督	系统创建	2022-12	-14 15:18:33	宣誓		
	空权聚角色	用户自动初始化角色,无权限	系统包建	2022-12	14 15:18:36	没有		
~	newroke		请不要删除测试数据	2023-05	-09 17:42:46	1018	11 H	-
	test	123	请不要删除测试数据	2023-06	-30 14:18:03	55550	21	H
	仪任务管理		请不要删除测试数据	2023-05	-30 17:59:23	5055E	22	-
	自定义角色产品test		请不要删除测试数据	2023-07	-04 16:28:20	AND IN		-



5.3 组织单位管理

此模块主要用于对系统中的资产或用户进行分区域的权限划分,用户可根据自身组织结构、办公区域等维度自由分配组织单位和各级账号间的权限关系

5.3.1 组织单位树

作区	V	用产管理 2 组织单位管理						
和仪表盘								
195-92	*	组织单位结构树	深加用原料单位	默认工作区				
袋裙	<i>.</i>	haha		组织单位基本信息				
中心	×	- 默认工作区		编织单位名称	默认工作区			
99.28		PPEC		組织単位 Ю	1			
		 test2 test2 1 		相纲單位负责人	admin			
ξΦ0		 test2.1.1 		创建时间	2021-11-25 10:58:18			
10	\sim	test2.1.1.1		上次更新时间	2021-11-25 10:58:18			
1997		test1		子组织单位数	6			
				主机总数	455			
-16-18	1			城名总数	224			
航用户管理				服务资产总数	655			
产角色设度				Web 3社乐总融	377			
51 0 000				使权目标				
				管理员信息				
				周戸回	用户名	用户角色	最后登录时间	
				t.	admin	超级管理员	2021-12-27 18:37:49	

5.3.1.1 内容展示

组织单位管理页主要分为两个区,分别是左侧的组织单位结构树和右侧组织单位相 关信息展示:

组织单位结构树	章加根建织单位	默认工作区			
haha		组织单位基本信息			
- 默认工作区		组织单位名称	默认工作区		
 test2 test2.1 		组织单位 ID 组织单位负责人	1 admin		
 test2.1.1 test2.1.1.1 		创建时间 上次更新时间	2021-11-25 10:58:18 2021-11-25 10:58:18		
test1		子组织单位数 主机总数 绒名总数	6 455 224		
		服务资产总数 Web 站点总数 提权目标	655 377		
		管理员信息	田白北	田之命会	奉任帝 高时间
		1	admin	超级管理员	2021-12-27 18:37:49

● 组织单位结构树:



- 包含用户可见的所有组织单位展示以及对应层级关系树
- 组织单位层级向下无上限,用户可根据实际情况自由创建
- 组织单位相关信息展示:
 - 展示组织单位的基本信息,包括以下字段:
 - ◆ 名称
 - ♦ ID
 - ◆ 负责人
 - ◆ 创建时间
 - ◆ 更新时间
 - ◆ 子组织单位统计
 - ◆ 主机总数
 - ◆ 域名总数
 - ◆ 服务资产总数
 - ◆ web 站点总数
 - ◆ 授权目标
 - 展示具备组织单位使用权限的用户列表,包括以下字段:
 - ◆ 用户 ID
 - ◆ 用户名
 - ◆ 用户角色
 - ◆ 最后登录时间

5.3.1.2 组织单位添加

添加根组织单位,点击"添加根组织单位"文字按钮,填写组织单位的相应参数:



* 组织单位名称	请输入组织单位名称	
组织单位负责人	选择负责人,组织单位负责人默认为创建者	V
组织单位管理员	选择管理员 (可多选)	
授权目标限制②	域名可输入格式: www.chaltin.cn	
备注	请输入对组织单位的一些备注说明	

- 组织单位名称
- 组织单位负责人
 - 默认为创建人,具备组织单位的编辑、删除等管理权限
- 组织单位管理员
 - 默认为负责人的所有上级管理,具备组织单位的查看权限
- 授权目标限制
 - 授权目标可控制用户可扫描的目标权限,为空时表示不限制
- 备注



5.3.1.3 添加子组织单位

对根组织单位或其他已存在组织单位可创建其子组织单位。通过组织单位结构树选 中需要创建子组织单位的父级组织单位,点击"添加"按钮,填写相应参数即可创建子 组织单位:

组织单位结构树	海加根重出单位	默认工作区-PPEC			
haha		组织单位基本信息			
 默认工作区 		组织单位名称	默认工作区-PPEC		
PPEC Alta state into		组织单位 (D	8		
 test2 test2 1 		组织单位负责人	admin		
+ test2.1.1		创建时间	2021-12-21 16:34:27		
fest2.1.1.1		上次更新时间	2021-12-21 16:34:27		
test1		子组织单位数	0		
		主机总数	0		
		城名总数	0		
		服务资产总数	D		
		Web 站点总数	0		
		授权目标			
		管理员信息			
		用户 ID	用户名	用户角色	最后登录时间
		1	admin	超级管理员	2021-12-27 18:37:49

添加流程同 5.3.1.2 组织单位添加。

5.3.1.4 组织单位编辑

通过组织单位结构树,选中要编辑的组织单位,点击"编辑"按钮,变更相应参数即可:修改完毕后,点击"确认",改动参数即生效若点击取消或右上方的"×",则改动不会生效。

组织单位结构制	海加林组织单位	默认工作区-PPEC			
haha		组织单位基本信息			
- 默认工作区		组织单位名称	默认工作区-PPEC		
PPEC III III III		相积单位 (D	8		
 test2 test2.1 		组织单位负责人	admin		
* tost2.1.1		创建时间	2021-12-21 16:34:27		
test2.1.1.1		上次更新时间	2021-12-21 16:34:27		
test1		子组织单位数	0		
		主机总数	0		
		城名总数	0		
		服务资产总数	0		
		Web 站成总数	0		
		授权目标			
		管理员信息			
		用户 ID	用户名	用户角色	最后登录时间
		а.	admin	超级管理员	2021-12-27 18:37:49



* 组织单位名称	PPEC	
组织单位负责人	admin	V
组织单位管理员	admin ×	
授权目标限制⑦	域名可输入格式: www.chaitin.cn	
备注	维护世界和平	

5.3.1.5 组织单位删除

组织单位结构树	漆加根纸粉单位	默认工作区-PPEC			
haha		组织单位基本信息			
- 默认工作区		组织单位名称	默认工作区-PPEC		
PPEC III SAM III		相助和命位 (D	8		
= test2		组织单位负责人	admin		
- test2.1.1		创建时间	2021-12-21 16:34:27		
test2.1.1.1		上次更新时间	2021-12-21 16:34:27		
test1		子组织单位数	0		
		主机总数	0		
		城名总数	0		
		服务资产总数	D		
		Web 站成总数	0		
		授权目标			
		管理员信息			
		用户 ID	用户名	用户角色	最后登录时间
		1	admin	超级管理员	2021-12-27 18:37:49

说明:

删除正在被使用的组织单位会影响组织单位下的用户查看、操作对应资产、引擎等的权限,建议删除前仔细检查是否有绑定的用户和引擎,修改后再进行删除。



5.3.1.6 组织单位切换

在左侧的二级导航栏上会显示用户当前所处的组织单位维度,点击"下拉"按钮可选择用户可见的所有组织单位并切换视角:

<->洞鉴x-	RAY							admin
默认工作区	×	用产资理 / 组织单位管理						
の 金局仪表盘								
日初時開発	×	组织单位结构树	深加市场积单位	haha				
A 最终教育	<i>.</i>	haha		组织单位基本信息				
素 液产中心	×	▶ 默认工作区		编织单位名称	haha			
* ж лен	2			組织単位 10	2			
th annexes.				组织单位负责人	admin			
m watches				包據时间	2021-11-25 11:12:11			
目 如如本	×			上次更新时间	2021-11-25 11:12:11			
② 系統管理				子组织单位数	0			
5 BOTH				主机总数	27			
				城名总数	0			
系统用户管理				服务资产总数	25			
用产角色设置				Web 95/5/028	5			
-				授权目标				
				管理员信息				
				用户的	用户名	用户角色	最后要录时间	
				114	test	系统管理员	*	
				×	Ray XR-510 21 11 301 /10 0 2021	Chalton Tech.		

说明:用户在不同组织单位下具备不同资产和引擎的查看或管理权限

5.3.1.7 组织单位视角数据查看

在组织单位基本信息中,点击主机总数、web站点总数可切换至目标组织单位后, 展示 对应资产列表:

组织单位结构树	海加根紙供单位	默认工作区-PPEC			
haha		组织单位基本信息			
- 默认工作区		组织单位名称	默认工作区-PPEC		
PPEC III.II SHI III.N		组织单位 ID	8		
+ test2		田初始合作市人	admin		
 test2.1 		30.914 (at)40475			
 tost2.1.1 		创建时间	2021-12-21 16:34:27		
test2.1.1.1		上次更新时间	2021-12-21 16:34:27		
test1		子组织单位数	0		
		主机总数	0		
		城名总数	0		
		服务资产总数	o		
		Web 站成总数	0		
		授权目标	_		
		管理员信息			
		用户 ID	用户名	用户角色	最后登录时间
		1	admin	超级管理员	2021-12-27 18:37:49

六、个人中心模块

6.1 个人中心

点击界面的右上角用户名,出现下拉菜单,点击"个人中心",即可进入个人中心页面。

以工作区 ☆ ^{房仪表盘}	2 2	周仪表盘									R 个人中心 JF Open AP
日期管理 基成管理 資产中心	• •	今日新增漏	^{两数}	待修复漏洞总数	417	待修复绑口	1今選調总数 84	今日已修订	(漏洞数 <mark>()</mark>	已修复瀕洞总数	о жн 0
K 約管理	2	待分配漏洞墙	长率: 100.0%	高总及以上占比:	5.1%	当日新場録	1令数:0	已修复演习机	崔长率: 0.0%	平均漏防修复时间]-
和表中の 知花床 系統管理 馬売用学管理 馬売用学管理 用产角色设置 単気中位筆環	*	资产运行情,	2	 這行中 等机中 未知 	141 264 50	资产数量统计 资产总数 主机资产数 Veob 资产数 未知风险资产 不存活资产数	832 455 377 52 31.7%	资产		 萬電波/ 中電波/ 中電波/ 中電波/ 中電波/ 中電波/ 生電波/ 未知道/ 	 m 163 m 44 m 120 m 453 m 52
		风险资产组	訳单位 Top 5				业务系统	漏洞排名 Top 5			
		排名	组织单位	资产总数	展示总数	影响资产数	排名	业务系统	资产总数	展現総数	影响资产数
		.1	联认工作区	829	34419	327			11.2.2.5		

个人中心页面主要展示当前用户的个人信息,包括个人基本信息、和登陆选项的设置。

6.1.1 个人基本信息

个人基本信息展示当前登陆用户的用户名、用户 ID 和创建时间。

- 用户名: 创建当前用户时设置的用户名称
 - admin 用户为系统预设用户
- ID: 创建当前用户时产生的唯一 ID
- 创建时间: 创建当前用户的时间



admin 1 2021-11-25 10:58:18 2021-12-27 18:31:53 超級管理品 - - -
admin 1 2021-11-25 10:58:18 2021-12-27 18:31:53 超級管理员 - - -
1 2021-11-25 10:58:18 2021-12-27 18:31:53 細級管理员 - - -
2021-11-25 10:58:18 2021-12-27 18:31:53 超感管理派 - - -
2021-12-27 18:31:53 超級鞭理品 - -
超级管理员 - -
- - -
 数据估计 全部化误差。 任务情理 任务情理 任务情理 任务情理 优务成计 任务情理 优务成功 新聞 日間能量 激励 1日能量 教育 日間能量 教育 日間能量 教育 私情報 生成服表 常務後 私情息 生成服表 常務後 未成長数

6.1.2 登录选项

登陆选项展示当前用户的登陆设置。

若用户为密码登陆,在此处可以修改密码,具体操作为:

- 点击密码登陆右侧的 "修改密码" 按钮
- 弹出密码修改页面。用户输入当前密码、新密码和确认新密码
- 点击确认,系统提示 "密码修改成功", 跳转到登陆页面

盤奏选项	
密码登录	修改面印

修改密码		×
*旧密码	请输入用于登录系统的当前密码	
* 新密码	请输入用于登录系统的新密码	
*确认新密码	请输入用于登录系统的新密码	
	EX	消确定



6.1.3 动态身份验证

可以选择开启默认关闭的动态身份验证。

<・>洞鉴x-	RAY	admin
默认工作区	V	个人中心
© 全局仪表盘		 ▼ 用户管理 ▼ 系統用户管理
日 扫描管理	3	添加和解鍵 翻錄
』 基场管理	×	- 用户角色设置 添加和编辑
\$ 资产中心		制除 - 组织单位管理
△ 漏洞管理	×	添加印編辑 删除
直 报表中心	×	 基线管理 基线检查任务
□ 蛀识库	Ŷ	运动和 (1) 编辑 制章
③ 系統管理	Ŷ	管理的组织单位 测试流动组织单位171373964
△ 用户管理	^	
系统用户管理		堂朱道明
用户角色设置		老得登录 (修改进码
相积单位管理		动态身份输证
		动态身份验证设置
		X-Ray X01-60(4) 10-34-05-001_113-0-5024-05abits Tach.

初次使用时候通过输入登录密码进入设置界面。可以使用手机APP(手机APP store 或应用商城搜索"Auth"或者"动态身份验证",如 Authy、OTP Auth、Google Authenticator)扫二维码添加私钥到手机认证应用。后每次通过密码登录后还需要查 看认证 APP 并填写六位数动态验证码才能继续访问系统。



< →洞墨x-							admin
默认工作区	×	个人中心					
© 全路仪表盘			 用户管理 系统用户管理 	动态身份验证		×	
	3		添加和編 副除		66920		
d assign	×		 用户角色设置 添加和線 				
意 Ⅲ户中心	÷		新設 ・ 組织単位第5				
4 派羽管理	π.		添加和編 創編				
⑧ 报表中心	÷		 基线管理 基线检查任! 				
C SURF	٠		活加和编 删除	D S P S C			
⑤ 系统管理	*	管理的组织单位	制试剂加组织	请使用手机动态身份验证 APP 扫描	l该二维码添加密钥后进行验证	E	
△ 用/◎管理	0		. W.W.T.D.FF	*动态身份验证码 情绪入据定担任的7		_	
系统用户管理		登录选项					
HPABUE		密码登录				聯定	他改进场
编织单位繁荣		动态身份输证					
		动态身份验证设置					
				x-Hay XTI-B	H 19-24.05.001_15 @ 0024 Own	Im Tech	

如想关闭动态身份验证设置,点击关闭并填写系统登录密码校验通过后关闭。

6.2 Open API

点击界面的右上角用户名,出现下拉菜单,点击 "Open API",即可进入 Open API 页面。

认工作区	× 9	用仪表盘									名 个人中心	
 2米G表盘 1)振客理 最低管理 第产中心 風彩管理 		今日新增潮	月数 〇 长率: 100.0%	待博复课网总数 34417 高色思以上cttr.51%		特修复群口令灌溉总数 84 当日影谱41口令数:0		980 E#8	- 今日已修复漏消数 0 已修复属闭锁长梁: 0.0%		■ Convert ■ Convert ● 201 ● 201 ■ Convert	
相表中心 如花輝 系代管理 用户質理 系式用户質理 用户角色设置 単に用の世界	* * *	资产运行情		 进行中 伊松中 未知 	141 264 50	资产数量统计 资产总监 主机资产数 Web 资产数 未知风险资产 不存活资产数	832 455 377 52 31.7%		() 一次の時間の時間の時間の時間の時間の時間の時間の時間の時間の時間の時間の時間の時間の	 再优担 中优担 4 化化 4 化 4 1 (1) 4 1 (17* 163 17* 44 17* 120 17* 453 17* 52	
盤於華位筆唯		风险资产组 排名 1	税単位 Top 5 組织単位 際以工作征	资产总数 829	建滚齿数 34419	影响直产数 327	业务系制 郑名	克圖洞排名 Top 5 业务系统	Bratt Batte	漏洞总数	影响资产数	

Open API 页面主要展示当前用户配置的 API。用户可以在此处查看、添加、编辑、 删除自定义的 Open API。

6.2.1 Token 展示

汇总了用户的全部 Token,并且提供可以查看 Open API 文档的接口。

6.2.1.1 内容展示

展示当前用户添加的所有 Open API, 次序从新到旧排列, 如下图所示:

适加一条 Open A	РІ	壹報 Open API
token: f4RxwiNe		特政 制度
有效期	2021-12-02 18:59:36 - 任期	
备注	2	
访问权限	允许任何人访问	
token: HWMkDE	35	1973 BUR
有效期	2021-12-02 18:59:35 - 长期	
备注		
访问权限	允许任何人访问	
oken: v2dsdnip		452X MIII
有效脏	2021-12-02 11:30:36 - 458	
番注	>	
防何权磨	ft许在何人比6间	
tokon: with dawl	1	10.00 mm

- 单个 Open API 展示信息包括:
 - token: Open API 的 token。Open API 添加后,将只展示 token 的前八 位, 其他位数加密处理
 - 有效: Open API 的有效期限。一个 Open API 的 toekn 只能在其有效期内 才能使用。token 过期后即失效,界面上将高亮提示过期


- 备注:用户为 Open API 添加的备注。因 token 加密展示,添加合适的备注 可以方便地使用户区分各个 Open API
- 访问权限:可访问该 Open API 的主机 IP 白名单。如果不设置访问权限, Open API 将允许任何人访问
- 可进行操作:用户可对 Open API 进行修改或删除的操作。详情可见下文修改 和删除的说明



6.2.1.2 添加 Open API

可以在此界面添加多个 Open API, 具体步骤为:

● 点击"+添加一条 Open API"按钮,显示配置相应信息的弹窗;

+ 添加一条 Open A	R	查看 Open API 文档
token: f4RxwiNe		· #22、第38
有效期	2021-12-02 18:59:36 - 长期	
俗注	3	
访问权限	允许任何人访问	

配置基本信息:

■ 过期时间, 配置 Open API 的过期时间, 有填写、选择两种设置方法:

◆ 填写过期时间,时间格式为 yyyy-MM-dd HH:mm,例如:2018-10-17
 10:28;

- ◆ 选择过期时间:
 - ✤ 点击输入框,在出现的下拉菜单中选择日期;
 - ◆ 点击"选择时间",在出现的下拉菜单中选择时间。
- 备注,可在此为 Open API 添加自定义的备注:
 - ◆ Open API 添加后, token 将加密展示, 添加合适的备注可以方便用户区 分各个 Open API。



基本信息	2 访问权限设置	3 信息确认
🥚 请填写	Open API 的基本信息,token 从创建成功开始生效	
计期时间	为空表示无限期	Ē
75,40,63 (6)		

- 点击"下一步",配置访问权限:
 - 选择是否启用 IP 白名单:
 - ◆ 若禁用 IP 白名单, Open API 将没有访问限制, 允许任何人访问;
 - ◆ 若启用 IP 白名单, 需填写 IP 白名单:
 - ◆ 只有 IP 白名单上的 IP 方可访问该 Open API;
 - ◆ 多个 IP 间以换行分隔。

添加一条 Open API	×
基本信息 适向权限设置 访问权限设置	③ 信息确认
😑 IP 白名单处于关闭状态时,访问没有任何限制	
IP 白名单 (关词)	
	上一步

- 点击"下一步",确认信息:
 - 在生成 token 前最后确认配置的过期时间、备注和访问权限是否无误。



→ 基本信息 -	访问权限设置	3 信息确认
😑 请确认以下	信息是否正确,确认无误,请点击完成生成相应的 token	
过期时间	长期	
备注	-	
访问权限	允许任何人访问	

- 点击"完成", Open API 生成成功, 界面将展示 token 和配置信息。
 - 点击 token 旁的"复制"按钮可以一键复制 token;
 - 注意:token 只在此界面显示一次,界面关闭后,软件将再也不会显示 token。 请务必在此页面复制好 token,并妥善保存。

Open API	token 已生成,本页面关闭后,将不再显示 token,请妥善保存	
Token	复制	
有效期	2021-12-23 16:21:33 - 长期	
备注	±	

- 点击"已完成复制保存,关闭当前页面"或弹窗右上角的关闭,关闭界面;
- 回到 Open API 界面,显示该 Open API 已添加,并展示在所有 Open API 的最 上方。



6.2.1.3 修改 Open API

可在此界面修改已添加的 Open API, 具体步骤为:

找到需要修改的 Open API, 点击 Open API 右侧的"修改":

+ 添加一条 Open A	NPI	查看 Open API 文
token: f4RxwiNe	,	情改團隊
有效期	2021-12-02 18:59:36 - 长期	
衛注	3	
访问权限	允许任何人访问	

- 编辑需要修改的配置,编辑配置的方式与添加 API 时类似:
 - 过期时间,可编辑 Open API 的过期时间,有填写、选择两种编辑方法
 - ◆ 填写过期时间,时间格式为 yyyy-MM-dd HH:mm,例如:2018-10-17
 10:28
 - ◆ 选择过期时间
 - ◆ 点击输入框,在出现的下拉菜单中选择日期
 - ◆ 点击"选择时间",在出现的下拉菜单中选择时间
 - 备注,可编辑 Open API 的备注
 - IP 白名单, 可编辑访问权限配置
 - ◆ 若禁用 IP 白名单, Open API 将没有访问限制, 允许任何人访问
 - ◆ 若启用 IP 白名单,填写或编辑已添加的 IP 白名单

◆ 只有 IP 白名单上的 IP 方可访问该 Open API

◆ 多个 IP 间以换行分隔



编辑 Open API		×
过期时间	为空表示无限期	Ē
备注	请设置 Open API 说明	li li
IP 白名单	关闭	
		取消 确定

- 配置完所有信息后,点击"保存"
- Open API 修改成功, 界面显示已修改的 Open API 信息
- 6.2.1.4 删除 Open API

可在此界面删除已添加的 Open API, 具体步骤为:

● 找到需要删除的 Open API, 点击 Open API 右侧的"删除":

添加一条 Open API		
ken: f4RxwiNe************		
有效期 2021-12-02	18:59:36 - 长期	
番注 -		
访问权限 允许任何人	方问	

- 在提示确认是否删除的弹窗中,点击"确认";
- 成功删除 Open API。



6.2.2 查看 Open API 文档

点击"查看 Open API 文档"按钮,可以跳转到 Open API 文档页面:

+ 添加一条 Open A	PI		查看 Open API 文档
token: f4RxwiNe			修改 副路
有效期	2021-12-02 18:59:36 - 长期		
衛注			
访问权限	允许任何人访问		

Open API 文档到具体使用方法请参考 Open API 文档。

6.3 登出系统

点击界面的右上角用户名,出现下拉菜单,点击"退出",即可退出系统,跳转至 登录界面。

NUTPE V 2002 ATTACK	<->洞鉴x-	RAY											
* 24324 * 24324 * 6458/38/78	默认工作区	V 5	2两仪表盘										名 个人中心
日 11年間 今日新聞期間 伊博男服為財 伊博男服為財 伊博男服為財 伊姆男加合教 9日伊男服為財 9日伊男服為財 伊姆男加合教 9日伊男服為財 伊姆男加合教 9日伊男服為財 伊姆男加合教 9日伊男服為財 伊姆男加合教 9日伊男朋友 0	◎ 全局仪表盘												dF Open API
2 8488 0 0 34417 84 0 0 70809399- 2 8094 0 0 0 0 18880-26-0 0 18880-26-0 0 198880-26-0 0 198880-26-0 19	E DAME	*	今日新增満課	國政	待修复漏洞总数		待修复象	口令運調总数		今日已修复漏消费	R.	已修复漏洞总	t C and
第 かやら 中 h H </td <td>A 基础管理</td> <td><i></i></td> <td></td> <td>0</td> <td>34</td> <td>417</td> <td></td> <td>84</td> <td></td> <td>1</td> <td>n</td> <td></td> <td>0</td>	A 基础管理	<i></i>		0	34	417		84		1	n		0
● 用空電 ● 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	素 预产中心	~		U	04	417		04			×		0
 ▲ RAPC ▲ RAPE ▲ RAPE<td>\$ MARH</td><td>*</td><td>待分配漏购增长</td><td>全事: 100.0%</td><td>高意及以上占比:5</td><td>.1%</td><td>当日新場</td><td>00□全限:0</td><td></td><td>已修复漏窍增长率。</td><td>0.0%</td><td>平均漏器修复时</td><td>ii) -</td>	\$ MARH	*	待分配漏购增长	全事: 100.0%	高意及以上占比:5	.1%	当日新場	00□全限:0		已修复漏窍增长率。	0.0%	平均漏器修复时	ii) -
日本時本 - <td>皇 根表中心</td> <td></td> <td>资产运行情况</td> <td>2</td> <td></td> <td></td> <td>谢产数量统计</td> <td></td> <td></td> <td>资产风险制</td> <td>级分布</td> <td></td> <td></td>	皇 根表中心		资产运行情况	2			谢产数量统计			资产风险制	级分布		
A 品報報 A 加加 A M 加 A M 加 A M 加 A M 加 A M 加 A M 加 A M M A M	13 maa	*					资产工程	832					
▲ 用用電理 新用用管理 用用曲台程 服用曲台程 服用曲台程 服用曲台程 服用曲台程 服用曲台程 服用曲台程 工作法 化石 Top 5 新程 信仰位 1 取以工作法 自29 34419 327	© 54993	~	_		· 189740	141	主机资产数	455				 高危资 中危资 	163
ARR/P 18/2 中水和 50 未知度地面下 52 中水流の下 52 用作曲台语者 用作曲台语 不作法用作用 52 不作法用作用 52 用作曲台语者 日本 日本 日本 1.5% 1.5% 月始音作曲目 日本 日本 日本 日本 1 田以下作法 829 54419 527 日 日以工作法 829 54419 527	二 局户管理	0			• 伊机中	264	Web 资产数	377				 任危法 	() ^a 120
APA1968년 田田中公理留	系统用户整理				◎ 未知	50	未知风险资产	52				· 安全社	i/* 453
E M R C T C C C C C C C C C C C C C C C C C	用户角色设置						不存活资产数	31.7%				 未知道 	J ^a 52
风险资产组织单位 Top 5 业务系统温润排名 Top 5 排名 组织单位 医产总数 漏涡总数 影响资产数 体名 法 第 通用总数 影响资产数 1 服以工作区 629 54419 527 1 第 1 1 1 1 <td>组织争位管理</td> <td></td>	组织争位管理												
排名 组织单位 脱产品数 展現品数 影响洗产数 排名 注外系统 脱产品数 展現品数 影响洗产数 1 取以工作区 829 34419 327 <td></td> <td></td> <td>风险资产组织</td> <td>Q单位 Top 5</td> <td></td> <td></td> <td></td> <td>业多</td> <td>6系统漏洞排名 Tr</td> <td>op 5</td> <td></td> <td></td> <td></td>			风险资产组织	Q单位 Top 5				业多	6系统漏洞排名 Tr	op 5			
1 NULFRE 829 54419 527			排名	組织单位	资产总数	展用品数	影响资产数	1	1名 业务	系统	资产总数	漏洞总数	影响资产数
NERS.			1	赋认工作区	829	34419	327						
如元政策													
											如无此道		