

极安 · 斥候

产品技术白皮书 V2.0



极安科技
JIAN TECHNOLOGY

浙江极安信息科技有限公司

二〇二四年二月

前言

版权声明

浙江极安信息科技有限公司版权所有，并保留对本文档及本声明的最终解释权和修改权。本文档中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明外，其著作权或其他相关权利均属于浙江极安信息科技有限公司。未经浙江极安信息科技有限公司书面同意，任何人不得以任何方式或形式对本手册内的任何部分进行复制、摘录、备份、修改、传播、翻译成其它语言、将其全部或部分用于商业用途。

免责声明

本文档依据现有信息制作，其内容如有更改，恕不另行通知。浙江极安信息科技有限公司在编写该文档的时候已尽最大努力保证其内容准确可靠，但浙江极安信息科技有限公司不对本文档中的遗漏、不准确、或错误导致的损失和损害承担责任。

信息反馈

如有任何宝贵意见，请反馈：

邮箱：ssr@jiansec.cn

公司官网：www.jiansec.cn

公司：浙江极安信息科技有限公司

您可以访问极安科技官网 www.jiansec.cn 获得最新技术和产品信息。

前言	2
版权声明	2
免责声明	2
信息反馈	2
1. 背景	4
2 产品概述	5
2.1 产品介绍	5
2.2 产品功能	6
2.2.1 资产收集	6
2.2.2 漏洞探测	7
2.2.3 专项漏洞测试	8
2.2.4 在线应用	9
2.2.5 反连平台	9
2.2.6 指纹与漏洞文库	10
2.3 产品特色	11
2.3.1 自动资产扩充	11
2.3.2 漏洞探测最小化发包	11
2.3.3 丰富的在线应用	12
2.3.4 用户和群组管理体系	12
2.3.5 灵活部署与拓展	13
2.3.6 丰富且易拓展的规则库	13
2.3.7 操作可溯源	14
2.3.8 在线协作	14
2.3.9 项目通知	15
3. 产品部署方案	16
3.1 单机部署	16
3.2 集群分布式部署	16
4. 客户价值及应用场景	17
4.1 实时资产巡检与发现	17
4.2 准确、全方位量化安全风险	17
4.3 高效整合提升工作效率	17

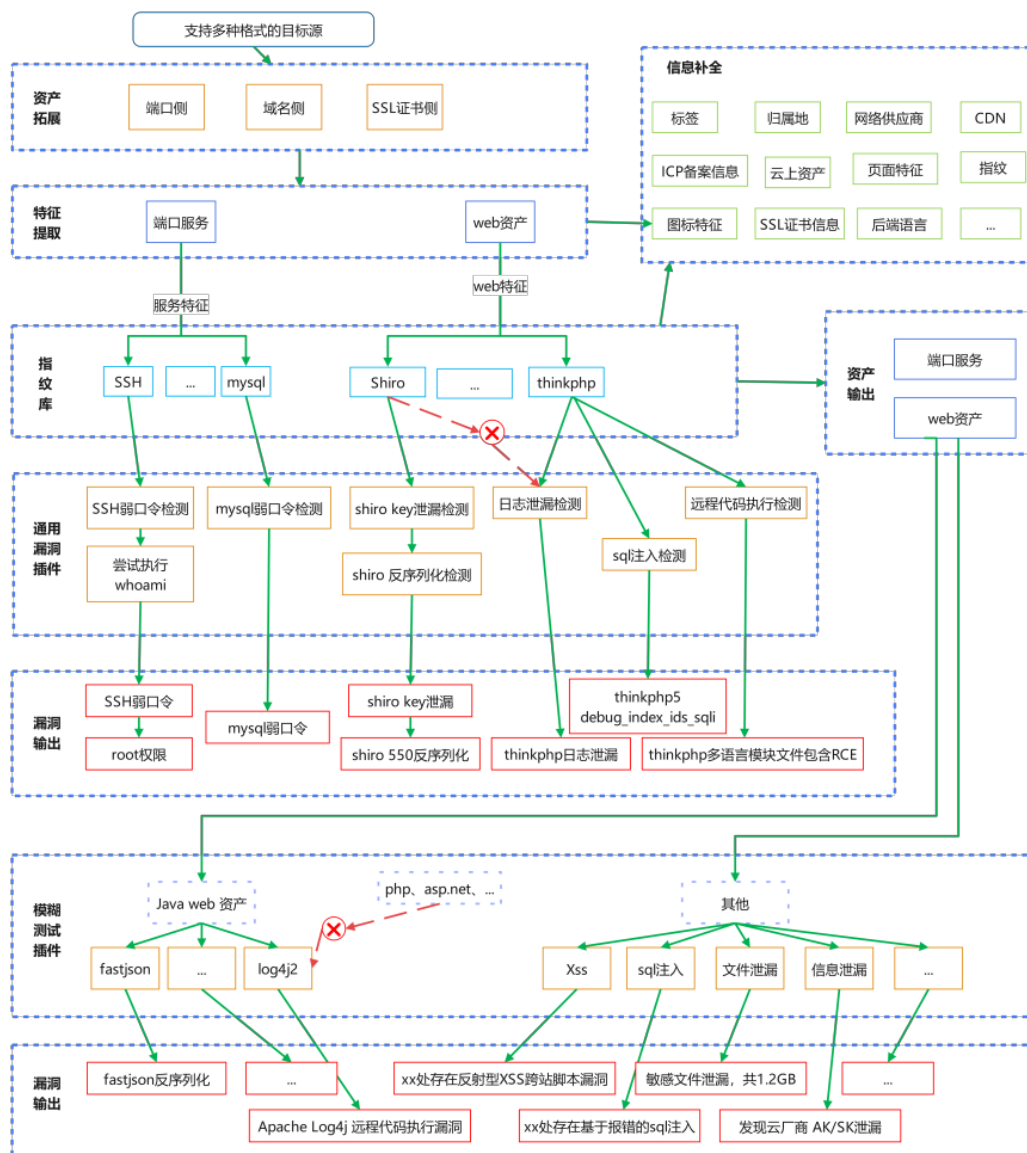
1. 背景

目前，网络安全建设仍以资产为中心，采用在外围进行威胁检测、安全防御等安全能力建设的方式，却忽略了资产自身的安全加固，导致近年来资产安全问题频发。从资产管理角度来看，随着 IT 架构的不断演变和系统应用方式的不断创新，IT 资产的种类和数量呈爆发式增长，资产状态频繁变动，资产定位困难。传统企业过去使用 Excel 手动登记管理的方式管理效率低下、易漏易错、响应时效长，已不适用于当今资产管理现状。从漏洞管理角度来看，传统基于主机漏洞和网络漏洞的扫描器均是通过漏洞逐项验证的方式对 IP 或网站进行扫描，效率低下，误报率较高。当风险发生时，很难在短时间内有效探测影响范围，拉长了风险扩散周期，造成威胁不能被第一时间处理，功能单一，不能满足快速发展的安全管理和技术发展需求。从攻击者视角来看，愈发扩大和分散的资产暴露面给企业带来了更多可侵入点。以往的安全防护虽然种类众多，但在侵入发生前也难以评估其有效性。当真实侵入发生后，一切都为时已晚。因此，我们急需一个能对企业的体系进行持续地有效性验证的工具，需要一个能尽可能真实模拟攻击产生的测试工具，能够将最真实、最完整的攻击面展露在用户面前，并在入侵前以评估报告提供的风险点为依据加固并修复暴露面。

2 产品概述

2.1 产品介绍

极安斥候(Choo)系统是由浙江极安信息科技有限公司自主研发的先进网络空间资产测绘与风险评估工具。本系统采取攻击者的视角，专业地为企业揭示隐藏的网络资产，通过综合漏洞风险识别、重要服务监测以及外部威胁情报分析，有效地监测企业的内网、外网及云环境资产。极安斥候致力于提供有效的安全解决方案，以帮助企业得体地应对新兴的安全威胁。



(图：斥候 (CH00) 综合项目逻辑)

2.2 产品功能



(图：斥候（CH00）产品功能架构图)

2.2.1 资产收集

斥候的资产收集功能是构建强大网络安全防线的首要步骤，它以自动化和智能化的特点，快速侦测和收集企业网络中的全部资产信息。首先，斥候展开对网络域名的彻底扫描，自动辨认并记录下主域名及其关联的子域名，为企业描绘一幅全面的网络资产分布图。接着，斥候深入到网络架构的每一个角落，对网站服务器、数据库、中间件等关键资产进行详细探查。它不仅能够精准识别各类资产的具体位置，还能发现服务版本、配置信息等关键数据，这些信息对于评估潜在的安全风险至关重要。

资产的深入剖析还包括了对操作系统的辨识、对网络设备开放的端口和服务的检测，以及对各种应用程序和协议的识别等，这些被收集到的数据项集成在斥候的数据库中，方便安全专家进行随后的漏洞评估和威胁监测。通过这样的资产收集，斥候不仅极大地提高了安全评估的起始效

率，同时也为深入的安全检查和风险管理打下了坚实的基础。这样一来，企业可以对内部网络的安全状况有一个清晰的认识，为制定更加有效的安全策略和措施提供了依据。

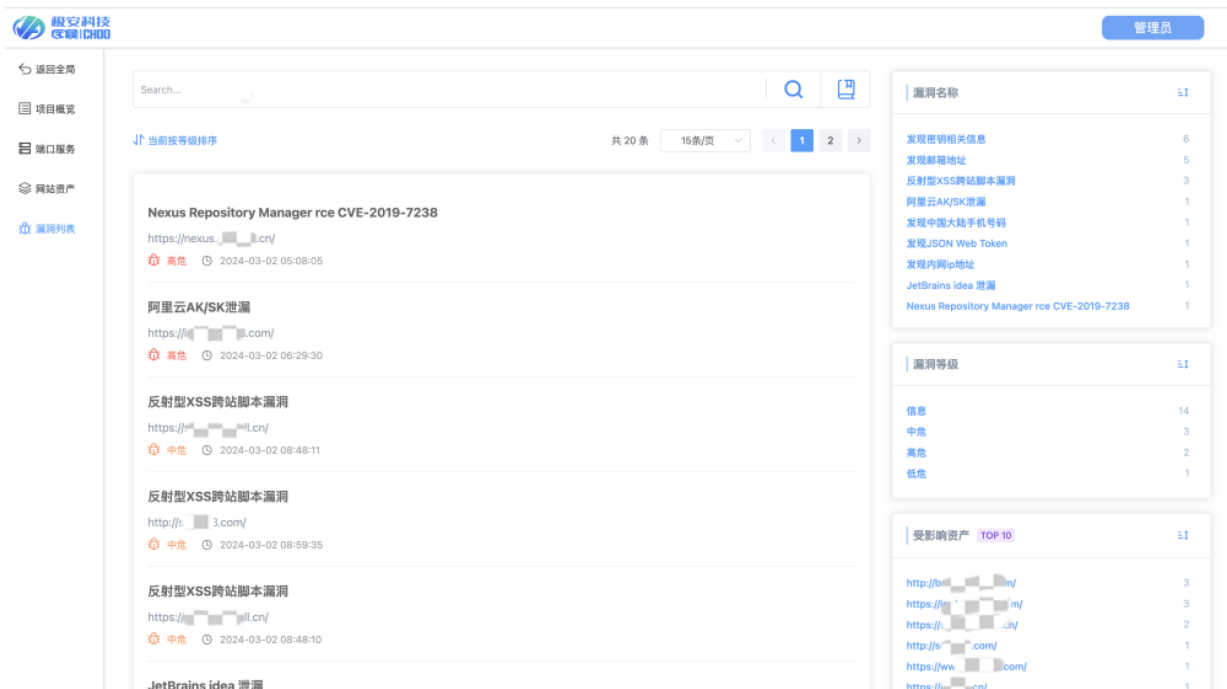
2.2.2 漏洞探测

使用高级搜索算法和漏洞数据库，斥候可以快速探测已知漏洞。这一过程由智能指纹识别技术辅助完成，确保漏洞探测的准确性和效率性。

对资产安全带来威胁的因素主要集中在漏洞以及一些高危的资产特征，所以识别历史上影响较大的高危漏洞对目前资产的影响，以及对一些已经列为高危特征进行定位和管理是资产安全风险管理的基礎。斥候集成众多历史上影响巨大的高危漏洞，尤其是一些容易被利用漏洞检测POC，可以对网络空间资产风险进行基础的排查和管理。

当新漏洞爆发，斥候会根据漏洞对企业客户资产的影响大小和范围进行评估，对影响较大的漏洞，持续投入研发力量进行无损检测程序的开发，尽快将无损检测程序集成进斥候。企业客户只需一键更新规则库，就可以在全部资产中进行存在此漏洞的资产检测，获知关注重点资产是否存在此漏洞，同时定位此漏洞究竟存在于哪些资产。管理人员可以通过斥候提供的SQL注入、XSS、RCE等漏洞验证信息的响应体和请求信息进行漏洞的验证，进一步确保检测结果的有效性，更有针对性的进行漏洞的修复操作。

在进行逐一的资产修复操作后，管理人员可以再次进行扫描操作，确认修复操作是否成功，完全消除漏洞给资产带来的风险。



2.2.3 专项漏洞测试

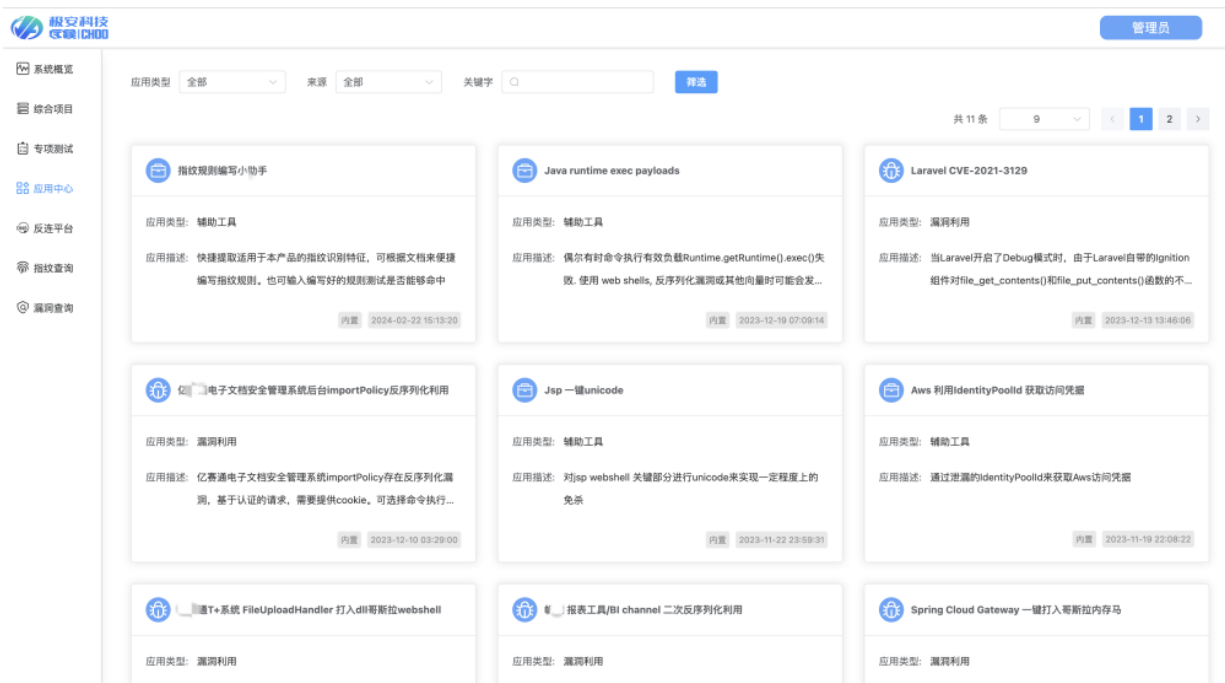
斥候的能力远不止于基本的漏洞探测，它还兼具专项测试的功能，提供了更深层次的安全保障。在网络安全领域，针对性的漏洞测试往往能够揭示那些通用方法可能遗漏的风险点。以国际上流行的log4j漏洞为例，斥候能够执行专项脚本对该类漏洞进行精细化测试。这种针对特定漏洞的深入探测，可以确保即使是在复杂且多变的网络环境中，潜藏的漏洞也无遁形。

除了针对知名漏洞的精确检测，斥候还支持自定义的漏洞测试功能，这使得安全团队能够根据实时的威胁情报或最新发现的漏洞，快速编制并执行测试脚本。这意味着当下一个log4j级别的重大漏洞出现时，斥候能够迅速适应新的安全检测需求，为网络安全防护提供加强版的保护层。



2.2.4 在线应用

为了更好地提高工作效率，斥候集成了丰富的在线应用，如利用框架和辅助工具，将原本杂乱无章的各种工具集成到了平台中，极大地简化了安全检测工具的使用和管理。



2.2.5 反连平台

反连平台允许安全研究人员和测试人员模拟 Web 应用在遭受攻击时可能会尝试建立的外部连接。在正常情况下，一些安全漏洞，如服务器端请求伪造（SSRF）、远程文件包含（RFI）、SQL 注入等，可能会导致 Web 应用尝试与攻击者控制的服务器或服务建立非预期的网络连接。通过斥候的反连平台，测试人员可以设置监听端点，然后通过构造的攻击载荷引导目标 Web 应用与这些端点建立连接。一旦建立了连接，反连平台就能捕获并记录相关的请求数据，从而帮助确认漏洞的存在和特性。

DNSLOG 反连平台


可选域名:

当前子域名:

[获取子域名](#)
[获取结果](#)

DNS 请求记录

☐ 打开此选项以自动刷新结果。

#	记录	IP	时间
2	test.234ca7ff.  js.	10.0.0.1:4052	2024-03-02 14:46:03
1	aaa.234ca7ff.  3.	10.0.0.1:61893	2024-03-02 14:45:00
0	ds.234ca7ff  4.	124.0.0.1:7360	2024-03-02 14:44:54

2.2.6 指纹与漏洞文库

斥候提供在线查询已收录的指纹规则以及漏洞名称。基于极安科技与 WgpSec 团队多年对漏洞检测和程序开发的积累，斥候内置了近年来具有重大影响的漏洞检测插件，这一特性完全符合企业级用户在资产基础安全方面的需求。针对 SQL 注入、XSS、RCE 等 0day、1day 漏洞，斥候提供了详尽的验证信息，便于企业用户自主进行漏洞确认工作。通过斥候在真实环境中的应用观察，发现弱口令问题普遍存在于许多系统服务中，因此，斥候 CHOO 特别增强了弱口令检测功能，并且拓展了包括 SSH、MYSQL、FTP、Postgres、MSSQL 等端口服务的检测。随着持续对新漏洞的发现和检测技术的不断积累，斥候将持续扩充其漏洞库，确保企业客户能够及时获得对新型漏洞的检测能力。

极安科技
JiAnTech

系统概況

综合项目

专项测试

应用中心

反选平台

指纹查询

漏洞查询

来源

全部

关键字

筛选

共 616 条

15条/页

1

2

3

4

5

6

...

42

>

	名称	网站	来源	收集时间	
1	WordPress Themes Brick...	Bricks Builder是一款用于WordPress的开发主题，提供直观的拖放界面，用于设计和...	https://bricksbuilder.io/	内置	2024-02-27 23:27:37
2	F5 BIG-IP Configuration ...	F5 BIG-IP Configuration Utility，是F5 BIG-IP平台中的一个重要组件。它允许用户通...	https://www.f5.com/	内置	2024-02-26 11:01:13
3	cPanel 主机管理面板	cPanel主机管理面板是一款强大且用户友好的网站托管控制面板，提供直观易用的界...	https://cpanel.net/	内置	2024-02-26 03:42:59
4	cPanel Webmail	cPanel Webmail是一种基于网页浏览器的电子邮件服务，通过cPanel控制面板轻松管...	https://cpanel.net/	内置	2024-02-26 03:40:09
5	Ghost CMS	GhostCMS是一款专注于内容管理的开源软件，可以帮助用户快速搭建个人博客网站	https://ghost.org/	内置	2024-02-23 04:41:45
6	用友U9	用友U9是一款集成化、智能化的企业资源计划（ERP）系统，助力企业实现数字化转型...	https://www.yonyou.com/	内置	2024-02-23 03:40:11
7	ConnectWise ScreenCon...	ConnectWise ScreenConnect 是一款远程控制软件，应用于全球 IT 管理服务提供商[...	https://www.screenconnect.com/	内置	2024-02-22 15:19:44
8	堡塔云WAF	堡塔云waf对网站业务流量进行多维度检测和防护,识别恶意请求防御未知威胁,阻挡SQ...	https://www.bt.cn/new/btwaf.html	内置	2024-02-22 13:50:33
9	华测监测预警系统	上海华测导航科技股份有限公司 华测监测预警系统	https://www.huace.cn/	内置	2024-02-18 22:56:13
10	华夏ERP	华夏ERP基于SpringBoot框架,立志为中小企业提供开源好用的ERP软件,目前专选销...	https://www.huaxiaerp.com/	内置	2024-02-18 22:37:47
11	西软云XMS	杭州西软信息技术有限公司 XMS云平台	https://www.foxhis.com/jypt.aspx	内置	2024-02-18 21:24:11
12	ZOHO ManageEngine Se...	ZOHO ManageEngine ServiceDesk是一个综合性的IT服务管理软件，提供了自动化工...	https://www.zoho.com/	内置	2024-01-21 14:03:51
13	ZOHO ManageEngine Op...	ZOHO ManageEngine OpManager是一个综合性的网络监控软件，用于管理网络、服...	https://www.zoho.com/	内置	2024-01-21 13:28:47
14	ZeroShell防火墙	zeroshell作为一款基于Linux的路由器、防火墙和VPN平台,具有强大的管理控制和安全...	http://www.zeroshell.org/	内置	2024-01-19 20:06:27
15	ClickHouse-client	ClickHouse是一个用于联机分析(OLAP)的列式数据库管理系统(DBMS),由俄罗斯排...	https://clickhouse.com/	内置	2024-01-19 19:58:12

2.3 产品特色

2.3.1 自动资产扩充

斥候系统在资产识别和漏洞扫描方面采用了先进的技术和策略，显著提升了传统扫描器的工作效率和准确性。与常规的安全扫描工具相比，斥候的方法论更加智能和高效，它能够从仅仅一个根域名出发，自动扩展和精细化整个网络资产的清单。

斥候利用高级语法和自动化机制，能够通过一个给定的根域名启动广泛的资产发现过程。这个过程包括 IP 反查域名、子域名爆破、DNS 解析等多种策略。通过 IP 反查，斥候能够识别出同一个 IP 地址关联的所有域名；通过子域名爆破，可以发现并列出一个主域名下所有可能的子域名；而通过 DNS 解析，斥候能够确定哪些域名是活跃的，以及它们对应的 IP 地址。

这些策略共同工作，使得斥候能够建立起主机资产、域名资产、网站资产之间的全面联系。这不仅包括发现一个 IP 地址下的所有网站，还包括揭示一个根域名下的子域名，甚至是网站内部的多级目录结构。这样，斥候为用户提供了一个全面的网络资产清单，这个清单不仅广泛，而且关联紧密，为进一步的安全分析和漏洞扫描奠定了坚实的基础。

在建立了全面的资产清单之后，斥候继续对目标系统进行深入的漏洞扫描和信息收集。利用先进的扫描技术和丰富的安全数据库，斥候可以有效地识别和评估目标系统中存在的安全漏洞、配置错误、敏感信息泄露等安全问题。这一过程不仅基于斥候已经建立的网络资产清单，还结合了其智能化的漏洞检测机制，确保了扫描结果的准确性和实用性。

总之，斥候通过其高效的资产识别机制和精准的漏洞扫描能力，为用户提供了一个从资产发现到安全评估的一体化解决方案。这不仅大大提高了安全团队的工作效率，也提升了整个网络安全管理的准确性和有效性。

2.3.2 漏洞探测最小化发包

斥候系统在设计上充分考虑了效率和精确性，特别是在漏洞探测的实现上。区别于传统扫描器常见的盲测模式，即在扫描开始时就向目标发送大量请求包以尝试不同的漏洞，斥候采取了一种更加智能和节约资源的方法。

在斥候系统中，所有的通用漏洞检测工具（PoC）都与特定的应用或服务指纹相关联。这意味着漏洞探测活动只会在系统先前成功识别出相关服务或应用指纹的情况下执行。例如，如果一个特定的漏洞检测工具是针对特定版本的 Apache 服务器设计的，那么该工具只会在斥候系统确认目标服务器运行着对应版本的 Apache 时被触发。这种方法极大地减少了不必要的网络请求，降低了对目标系统的干扰，同时提高了扫描的效率和准确性。

此外，斥候中的一些模糊测试插件同样遵循最小发包原则。以 log4j 漏洞检测为例，该插件不会对那些明显不运行 Java 后端的网站进行测试，比如那些使用 PHP、ASP.NET、Python 或 Golang 作为后端语言的网站。这种精细化的控制不仅进一步减少了无关紧要的网络请求，也降低了误报的几率，使得漏洞检测更加准确和高效。

斥候系统的这种设计理念有效地平衡了安全检测的全面性和目标系统的负载，避免了传统扫描工具中常见的资源浪费和潜在的服务中断风险。通过智能地将漏洞探测与服务指纹匹配，斥候确保了漏洞检测的过程既精确又高效，符合现代网络安全需求的发展方向。

2.3.3 丰富的在线应用

在当前的网络安全环境中，安全检测工具的多样性和复杂性常常导致管理上的混乱和更新同步上的挑战。这不仅增加了安全团队的工作负担，还可能导致安全漏洞和威胁检测的滞后。针对这一问题，斥候系统提供了一个创新的解决方案，通过将安全检测和运营中所需的各种工具转化为在线应用，极大地简化了日常使用和管理。

斥候的在线应用库提供了丰富的工具集合，覆盖了从资产探测、漏洞扫描到威胁分析等多个方面。这些工具被设计成易于使用的在线格式，用户可以根据自己的需求轻松选择和部署。通过将这些工具集成到一个统一的平台上，斥候使得用户能够在一个集中的地方管理和操作所有的安全检测工具，从而避免了传统安全工具分散管理的复杂性和低效率。

更重要的是，斥候支持官方规则的一键更新功能，确保所有在线应用都能及时同步最新的安全规则和检测算法。这一点对于维持高效的安全检测至关重要，因为它保证了工具能够及时识别和应对最新的安全威胁。用户不需要手动检查每个工具的更新，也不必担心使用过时的规则进行检测，斥候的自动更新机制完美解决了更新同步的问题。

此外，斥候还提供了定制化服务，允许用户根据特定的业务需求定制自己的安全检测规则和流程。这种灵活性进一步增强了平台的适用性，使其不仅适用于标准的安全检测场景，也能满足特定行业或企业的特殊需求。

总之，斥候系统通过提供一系列集成的在线应用和自动化的更新机制，极大地简化了安全检测工具的使用和管理。这不仅提高了安全团队的工作效率，也增强了企业对于网络威胁的防御能力，确保了企业资产的安全。

2.3.4 用户和群组管理体系

斥候系统的权限管理体系支持多用户和用户组，这意味着不同的用户可以根据他们的角色和职责被分配不同的权限。这种灵活的权限管理不仅提高了系统的安全性，而且确保了数据和资源的正确使用。

在这个体系中，管理员可以创建多个用户账户，并将这些用户划分到不同的用户组中。每个用户组都可以被赋予特定的权限集，这些权限集定义了组成员可以访问和操作的资源范围。这样，管理员可以轻松地根据业务需求和管理需求对用户进行权限划分和管理。

2.3.5 灵活部署与拓展

斥候系统的设计充分考虑了不同规模和需求的场景，提供了灵活的单机部署和集群部署选项，以满足各种应用场合。

单机部署是一个轻量级的解决方案，特别适合于需要快速部署的小型环境或临时任务。在这种部署模式下，斥候作为“移动地单兵武器库”，可以快速配置并立即投入使用，非常适合于需要快速响应或者在移动条件下工作的场景。这种灵活性使得单机部署成为在独立操作、内网探测或远程地点工作时的理想选择，即使在没有复杂网络支持的情况下也能使用。

集群部署支持横向扩展，用户可以根据业务需求非常方便地拓展探测节点。无论是在本地机房还是在公有云上，增加新的探测节点都只需一条命令，这极大简化了扩展过程，使得系统的扩展既快速又灵活。这种扩展能力不仅提高了斥候的数据处理能力和资源利用率，还确保了在面对不断增长的数据量和复杂的网络环境时，系统的性能和稳定性得到保障。

此外，集群部署还支持跨地域的数据集成和分析，这对于需要进行大规模网络监控和数据分析的组织尤其重要。无论探测节点分布在何处，斥候都能确保数据的实时收集和处理，为用户提供全面的视角和深入的洞察。

总之，无论是单机部署的便捷和灵活，还是集群部署的强大和可扩展性，斥候都能提供符合用户需求的解决方案，确保在不同的环境和应用场景下，用户都能有效地进行数据分析和网络监控。

2.3.6 丰富且易拓展的规则库

斥候系统的设计不仅注重用户体验和系统安全性，还特别强调了系统的即时更新和个性化定制能力。为了确保用户能够及时应对新的网络威胁和漏洞，斥候官方团队定期发布更新，这些更新包括热门指纹、最新的漏洞检测 POC (Proof of Concept)，以及各种在线应用的增强。用户可以通过后台的一键升级功能轻松地将这些最新的安全特性和工具集成到自己的系统中，这种设计极大地简化了维护流程，确保了用户系统的实时保护和最新状态。

除了官方提供的更新外，斥候还提供了强大的自定义功能。用户不仅可以使使用官方提供的工具和功能，还可以根据自己的特定需求自定义指纹、编写自己的漏洞检测 POC，以及开发适合自己业务场景的在线应用。斥候官方支持这种定制化开发，提供了丰富且成熟的软件开发套件 (SDK) 以及简洁明了的开发文档，帮助用户更好地理解如何利用斥候平台进行个性化开发。

这种开放性和灵活性的设计不仅允许用户根据自己的需求定制和扩展系统，还鼓励了一个活跃的社区环境，用户可以分享自己的指纹、POC 和应用，从而共同提高整个平台的安全性和效

率。斥候的这种设计理念，即结合官方的定期更新与用户自定义的灵活性，确保了用户可以在一个动态发展的网络环境中保持先进的防御能力和高效的工作流程。

2.3.7 操作可溯源

斥候系统提供了一个全面和详细的日志记录功能，允许用户在后台轻松查看所有敏感操作的日志。这包括但不限于网络扫描行为、在线应用的使用记录、系统设置更改、用户登录和权限调整等。这种透明的日志管理机制不仅确保了所有敏感操作的可追溯性，还增强了系统的安全性和可靠性。

通过这个功能，管理员可以全面监控系统的操作历史，快速定位和分析潜在的安全问题。例如，如果存在未授权的扫描行为或不寻常的应用使用模式，管理员可以通过日志记录迅速发现并采取相应的措施。此外，这些日志也支持审核和合规性需求，帮助组织符合行业标准和法规要求。

斥候的日志系统设计考虑了易用性和功能性，用户可以根据日期、时间、用户、操作类型等多种条件筛选和搜索日志记录，这使得追踪和分析特定事件变得简单高效。此外，为了保护日志数据的完整性和安全性，斥候还实施了严格的访问控制和加密措施，确保只有授权用户才能访问这些敏感信息。

总之，斥候的后台日志查看功能提供了一个强大的工具，用于监控、分析和回溯系统中的所有敏感操作。这不仅有助于增强系统的透明度和可靠性，还为用户提供了必要的信息，以确保高效和安全的运维管理。

2.3.8 在线协作

在斥候系统中，考虑到协作的重要性，特别设计了一项功能，允许在多用户环境下便捷地邀请其他用户共同参与当前项目。这种设计不仅提高了项目的协作效率，还加强了团队之间的互动和信息共享。

通过这一功能，项目负责人或管理员可以一键生成邀请链接来邀请其他用户加入项目。这样的设计极大地减少了项目启动和团队组建的时间，提高了工作流程的效率。

此外，这种多用户协作模式支持不同角色和权限的设置，确保每个用户都能在他们被授权的范围内工作，保障了项目的安全性和数据的保密性。管理员可以根据项目需求和团队成员的专业背景，灵活分配不同的任务和权限，这样不仅能确保项目高效推进，还能充分利用团队成员的专长。

斥候系统的这一功能特别适合于需要团队协作的项目，如攻防演练红蓝对抗、或跨部门合作的任务。通过简化的用户邀请和管理流程，斥候确保了团队成员之间的无缝协作，极大地提升了整个团队的工作效率和项目的成功率。

2.3.9 项目通知

斥候还提供的灵活项目通知机制，旨在确保项目团队及时接收到所有关键信息，从而促进更有效的项目管理和团队协作。这个机制特别设计来支持包括但不限于资产探测完成、项目完成、高危漏洞发现等在内的一系列重要通知，确保团队成员能够在第一时间获得必要的信息，以便采取相应的行动或调整项目策略。

为了适应不同企业的工作习惯和沟通偏好，斥候系统的项目通知机制特别支持多种协同平台，包括钉钉、企业微信、飞书等。项目负责人可以根据自己的需要和团队的沟通习惯，灵活选择将通知发送到这些平台之一。这种多平台支持不仅提高了通知的及时性和可见性，还增强了团队成员之间的互动和响应速度。

通过将斥候系统与这些流行的协同平台集成，项目负责人和团队成员可以在熟悉的工作环境中接收重要通知，无需频繁切换不同的应用程序或服务。这样的集成提升了工作效率，确保了信息的流畅传递，同时也强化了团队的协作和问题解决能力。总之，斥候系统的灵活项目通知功能和多平台支持共同确保了项目的高效运行和团队的紧密合作。

3. 产品部署方案

3.1 单机部署

单机部署是斥候产品的一种基础和快速的部署方式，适合中小企业或安全团队进行小型网络环境的安全评估，亦可作为移动式单兵武器库使用。在单机部署方案中，所有的服务进程、数据库和分析工具都运行在同一台计算机或服务器上。这样的部署既减少了硬件成本，也简化了部署和运维过程。

斥候产品的单机部署只需满足最低的系统硬件要求，即可完成全部的功能部署，并立即投入使用。安装过程十分简便，用户通过几个步骤的指导即可快速完成配置和启动，可以在短时间内建立起一个高效能的网络安全检测环境。

3.2 集群分布式部署

针对大型企业和安全团队，极安斥候可实现更为复杂且高效的集群分布式部署。在这种方案下，斥候的不同功能模块可以分布在多台服务器上运行，利用负载均衡技术实现服务进程的合理调度，从而提高整个系统的扫描和分析速度，优化资源的使用效率。

集群分布式部署强调系统的稳定性和可扩展性，能够保证在网络资产数量巨大或扫描需求频繁的情况下，斥候仍然能够保持高性能和稳定运行。同时，该部署方案支持快速横向扩展，响应企业业务的快速增长和较大规模的安全检测需求。

安全评估、漏洞检测和风险分析的任务在集群分布式环境下能够并行进行，这对于需要处理大量数据和高并发任务的企业来说是一个显著优势。此外，故障转移和数据备份也可以通过集群管理来实现，确保了业务的连续性和数据的安全性。

通过灵活的配置和高度的可定制性，极安斥候在集群分布式部署方案下可以很好地融合到企业的现有 IT 基础设施中，成为企业安全防护构架中的重要一环。

4. 客户价值及应用场景

4.1 实时资产巡检与发现

斥候系统通过其自主的资产发现和智能化资产梳理功能，能够进行实时的资产巡检和发现，特别是在边缘资产方面，帮助企业揭示和管理那些通常难以发现的网络元素。通过这一过程，斥候不仅促进了企业的风险量化，还实现了资产的全面可视化，使企业能够更有效地识别、评估和应对潜在的安全威胁，从而保障整个网络环境的安全性和稳定性。

4.2 准确、全方位量化安全风险

斥候系统提供了一种从攻击者视角出发的全面网络安全分析和风险评估方法。该系统不仅分析网络系统的各个方面的安全脆弱性，而且能够进行统一的分析和风险评估。它实现了资产对象、资产属性以及漏洞库等信息的有效联动，从而使企业能够获得一个全面的、实时更新的安全风险视图。

4.3 高效整合提升工作效率

斥候系统通过将丰富的在线程序和安全检测工具集成到单一平台，有效地提升了工作效率并精简了安全工具的使用和管理过程。这种高效的集成调度可以帮助企业更便捷地处理各类工作任务，从而显著提升产品效率和操作便利性。