阿里云
漏洞扫描

产品简介

文档版本：20200708

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云文档中所有内容，包括但不限于图片、架构设计、页面布局、文字描述，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止：** 重置操作将丢失用户配置数据。
	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告：** 重启操作将导致业务中断，恢复业务时间约十分钟。
	用于警示信息、补充说明等，是用户必须了解的内容。	 **注意：** 权重设置为0，该服务器不会再接受新请求。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明：** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	单击**设置** > **网络** > **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令。	执行cd /d C:/window命令，进入Windows系统文件夹。
斜体	表示参数、变量。	bae log list --instanceid Instance_ID
[]或者[a|b]	表示可选项，至多选择一个。	ipconfig [-all|-t]
{}或者{a|b}	表示必选项，至多选择一个。	switch {active|stand}

目录

1 什么是漏洞扫描

阿里云漏洞扫描（CSS）是数字化转型中的最佳互联网扫描实践，可帮助您自动发现网站关联资产，并进行高效精准的自动化漏洞渗透测试和敏感内容监测等，保障上线前和线上应用环境的安全性。

漏洞扫描结合情报大数据、白帽渗透测试实战经验和深度机器学习，提供全面资产威胁检测，包括：

- 资产漏洞
- 安全违法违规内容（如暴力恐怖、涉政、色情内容等）
- 网页篡改
- 挂马暗链
- 垃圾广告

第一时间帮助您精准发现网站资产和关联资产存在的安全风险，避免遭受品牌形象和经济损失，同时满足等保合规要求。

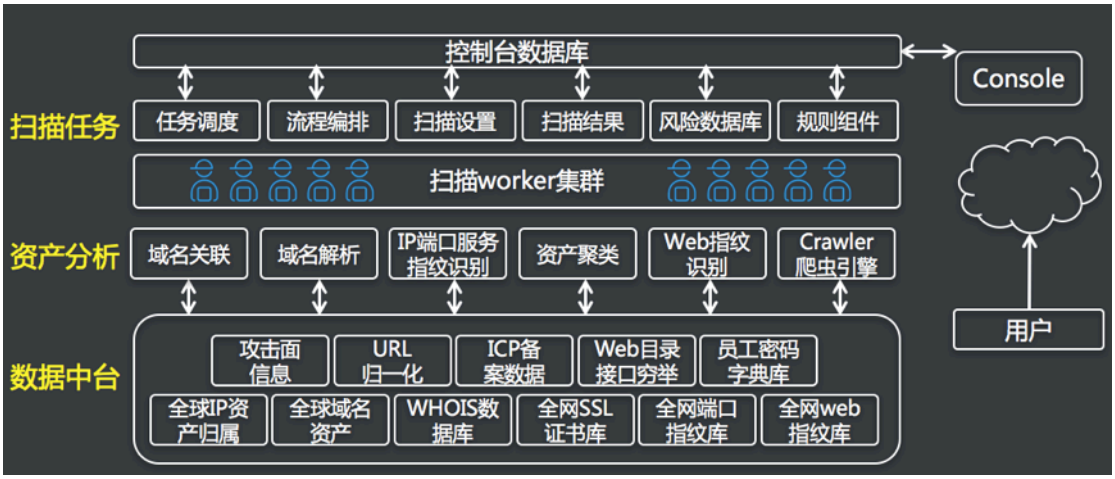
工作原理

漏洞扫描采用启发式2.0爬虫实现全面深度的页面爬取，使用具有渗透测试能力的漏洞检测插件帮助您全面检测安全隐患。同时内置多层验证规则，确保检测结果的高精准度，并提供详细的漏洞描述和解决方案帮助企业有效理解、验证、跟踪和修复漏洞，减少相关业务风险。

漏洞扫描支持网站内容风险和挂马篡改等检测。基于深度学习技术， 提供图片、视频、文字等多媒体的内容风险和挂马篡改智能识别服务，帮助您降低色情、暴力、恐怖等违规风险以及被黑客恶意篡改的风险。

2 产品架构

阿里云漏洞扫描由如下三大模块组成：



- **数据中台模块**：存储全网资产情报数据，包括全球IP资产归属、全球域名信息、WHOIS数据、全网SSL证书、全网端口指纹、全网web指纹、ICP备案信息、员工密码数据库等。
- **资产分析模块**：主要结合阿里云情报大数据，进行域名解析和关联，并分析和识别资产的IP端口服务指纹、web指纹等。
- **扫描任务模块**：由部署在阿里云的弹性可扩展扫描work集群完成，主要进行扫描任务配置、任务流程调度和编排，调用风险数据库和规则组件进行漏洞、敏感内容、挂马篡改等网站漏洞检测，并输出网站漏洞检测结果。

3 功能特性

本文档介绍漏洞扫描的功能特性。

全面发现关联资产

全面发现域名资产关联的子域名、Web服务器IP等，并提供详细的资产指纹信息，如中间件、应用程序、OS、端口、服务、地理、运营商等，让安全不留死角，防止跳板攻击。

深度专业的漏洞扫描

漏洞扫描可扫描以下漏洞：

漏洞类型	漏洞名称
弱口令检测	FTP、SSH、RDP、SMB、SMTP、POP3、IMAP、MYSQL、MSSQL、phpMyAdmin、MongoDB、MemCache、Redis、Oracle、PostgreSQL、Subversion、LDAP、PPTP、VPN、HTTP基础认证、HTML Form表单、Tomcat Web控制台。
Web注入漏洞	SQL注入、命令注入、代码注入、SSRF注入、表达式注入、反序列化、XXE注入。
文件包含漏洞	文件包含（LFI/RFI）、任意文件读取、任意文件上传。
前端漏洞	XSS、ClickJacking、Jsonp劫持、HTTP头注入CRLF、URL跳转。
错误配置	WebServer配置失误、中间件配置失误、容器配置失误。
信息泄露	配置文件、测试文件、目录遍历、备份文件、SVN、GIT、压缩包、临时文件、接口暴露、心脏滴血漏洞。

敏感、违规违法内容检测

全面智能发现网站涉黄、涉恐等敏感信息，防止您的品牌形象遭受损失。色情图片识别准确度高于90%。模型高度灵活，可根据您的要求实时调整生效。可识别武器、敏感人物、血腥场面、特定着装、特殊符号等暴恐社政文字、图片和视频，并根据时政热点和舆情事件快速更新。

篡改挂马检测

基于多种模型融合技术从多维度对您的网站进行实时监控，及时发现页面异常篡改和挂马，并第一时间进行告警和通知应急处理。

直观的风险扫描报告

针对扫描的结果形成专业的风险扫描报告。对扫出来的安全漏洞进行归类，并提出修复建议。

辅助风险验证和修复指导

提供安全专家级辅助漏洞验证和漏洞修复指导。

4 产品优势

本文档介绍了漏洞扫描的优势。

风险覆盖全

全面覆盖WEB漏洞、弱口令、涉政暴恐色情内容、网页篡改、挂马暗链、垃圾广告等各类网站风险。全面支持源码、文本、图片等内容格式。同时从白帽视角，全方位发现关联资产风险，避免关联资产成为您安全木桶的短板，影响整体安全效果。

检测准确高

采用深度启发式Web 2.0爬虫技术，基于动态解析，链接抓取更准、更全、更深。90%插件基于渗透测试经验开发，且内置多层自动验证规则，保证漏洞检测高准确率。采用综合决策技术、目标检测技术和模型记忆技术，确保内容风险精准命中。

响应速度快

采用集群式的弹性扩展架构，可按需快速扩展扫描引擎集群，实现扫描性能的弹性扩展。高速处理引擎，实现日处理图片十亿张，秒级响应发现敏感图片。业内一流安全专家，7*24快速响应您的安全需求，支持最新漏洞检测，同时帮忙您提供辅助漏洞验证和漏洞修复建议。

随时随地查

无需安装，开通账号，即可一键开启扫描之旅。无需人工升级，实时直接享用最新漏洞库和风险算法。可随时随地登录管理控制台，下发扫描任务，查看扫描进度和报表，实时获得扫描结果通知和告警。服务期内享受不限次数扫描。

5 应用场景

介绍漏洞扫描的应用场景。

资产变化监控

可自主常态扫描实时监控资产变化，包括子域名、IP、端口、服务、web组件等。

网站脆弱性风险评估

基于大数据信息情报积累，提供自适应智能的检测规则，实现全面的脆弱性风险评估。包括：网站上线前验收；网站日常安全评估；重大活动期间的网站安全评估。

违规内容监测

当您的网站内容涉及违规信息时，可为您提前预警并提供违规网页地址及快照查看功能，无需手动检测网站内容便可解决网站违规信息。

黑客挂马篡改攻击监测

提供首页检测服务和网页内容检测服务，帮助您实时检查您的首页是否具有被攻击、挂马、暗链、垃圾广告等风险， 并在发现遭攻击风险后第一时间通知您。