

ALIBABA CLOUD

Alibaba Cloud

漏洞扫描
用户指南

文档版本：20201014

 阿里云

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. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，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
 危险	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。	 危险 重置操作将丢失用户配置数据。
 警告	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。
 注意	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。
 说明	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。
<code>Courier</code> 字体	命令或代码。	执行 <code>cd /d C:/window</code> 命令，进入Windows系统文件夹。
<i>斜体</i>	表示参数、变量。	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] 或者 [a b]	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
{ } 或者 {a b}	表示必选项，至多选择一个。	<code>switch {active stand}</code>

目录

- 1.概览 ----- 05
- 2.扫描目标 ----- 07
 - 2.1. 添加资产 ----- 07
 - 2.2. 管理资产 ----- 08
 - 2.3. 搜索资产 ----- 08
 - 2.4. 资产助手 ----- 09
 - 2.5. 标签分组 ----- 09
- 3.扫描任务 ----- 11
 - 3.1. 限制条件 ----- 11
 - 3.2. 创建扫描任务 ----- 11
 - 3.3. 管理扫描任务 ----- 13
 - 3.4. 管理任务实例 ----- 14
- 4.攻击面透视 ----- 18
 - 4.1. 概述 ----- 18
 - 4.2. 攻击面数据查询 ----- 18
 - 4.3. 字段查询运算符 ----- 19
 - 4.4. 查询字段与示例 ----- 20
- 5.风险 ----- 24

1. 概览

漏洞扫描系统控制台的概览页面，助您快速进入各功能模块，及全面了解您资产的整体风险趋势、安全提升趋势及资产信息，具体包括：漏洞检测统计、待处理风险和已处理风险数量统计、资产概览、任务概览、扫描目标概览、任务实例概览、近期重要功能动态等。

概览页面展示以下模块：

- **风险与资产概览**：展示资产威胁程度（高危、中危、低危、信息）分布、高危漏洞数量、漏洞总数，及未扫描、巡检中和未巡检资产数量。



- 鼠标移动至左侧资产威胁程度分布图的不同颜色区域，可查看不同威胁等级的风险数量。
- 单击立即处理或漏洞总数下的数值，可跳转到[风险](#)页面，查看漏洞和内容风险详情并进行处理。
- 单击未扫描/巡检中/未巡检下对应的数值，可跳转到扫描目标 > 未扫描/巡检中/未巡检页面，查看相应的资产信息。
 - **未扫描**：展示未扫描资产，即未创建扫描任务的资产列表。建议您及时为未扫描资产创建扫描任务，并开启周期任务扫描，即对您的资产进行周期性安全巡检，助您及时发现并修复漏洞风险。
 - **巡检中**：展示已开启周期任务扫描的资产列表。您可对巡检中资产进行周期巡检，查看周期扫描结果及风险收敛趋势。
 - **未巡检**：展示未创建周期任务扫描的资产列表。您可对未巡检资产进行标签分组，并快速创建周期扫描任务。

- **风险处理概览**：展示了漏洞扫描检测到的最近7天内您资产中存在的风险统计数据，包括已处理和待处理的风险数量、不同危险等级的风险数量。

- **待处理风险**：展示最新的待处理、不同威胁等级（高危、中危、低危、信息）风险统计信息，及最近7天资产的风险总数趋势，助您了解资产的整体风险收敛趋势。

您可单击待处理风险下对应的等级风险统计数值，进入[风险列表](#)页，查看并处理风险，具体参见[风险](#)。

- **已处理风险**：展示最新的已处理、不同威胁等级（高危、中危、低危、信息）风险统计信息，及最近7天资产整体安全的提升情况，助您了解修复风险后资产的安全提升趋势。

您可单击已处理风险下对应的等级风险统计数值，进入[风险列表](#)页，查看已处理的历史风险漏洞详情。



在待处理风险区域，或已处理风险区域，从左至右移动鼠标，可查看最近7天待处理或已处理风险数量的变化趋势。

- **资产概览**：展示漏洞扫描授权检测的所有资产数量、阿里云资产数量及待确认授权管理的资产数量。



单击所有资产/阿里云资产/待确认下对应的数值，可跳转到扫描目标 > 所有资产/阿里云资产/待确认页面，查看相应的资产信息。

② 说明

- 开通漏洞扫描服务后，资产发现功能会自动发现并关联您云账号下已有资产，及后续新增资产，至待确认页面的资产列表中。
- 您需要及时对待确认资产进行确认、分组，并创建、开启扫描任务，避免遗漏资产遭受损失。

- **任务概览**：展示创建的扫描任务总数，及两种不同调度类型（单次任务、周期任务）的任务数量。

单击**单次任务/周期任务/任务总数**下对应的数值，可跳转到**扫描任务**页面，管理扫描任务和周期计划。

- **实例概览**：展示任务实例总数，及不同扫描状态（运行中、已停止、已完成）的实例数量。

单击**运行中/已停止/已完成/实例总数**下数值，可跳转至**任务实例**页面，查看不同状态的实例信息。具体可参见**管理任务实例**。

- **资产攻击面**：展示您资产中各个类型的攻击面统计数据。

- **近期重要功能动态**：罗列最新产品动态，如新功能发布、新漏洞检测插件集成等。

近期重要功能

单击一条记录名称可以查看其信息摘要和发布功能的描述信息。

相关文档

[升级和续费](#)

2. 扫描目标

2.1. 添加资产


开通漏洞扫描服务后，您首先要将网络资产以IP或域名的形式添加到扫描目标中。阿里云资产支持自动关联；非阿里云资产需要手动添加。

前提条件

已开通漏洞扫描。具体操作请参见[开通漏洞扫描](#)。

操作步骤

1. 登录[漏洞扫描系统控制台](#)。
2. 在左侧导航栏，单击扫描目标。
3. 根据您的资产是否属于阿里云资产，选择自动导入和手动添加操作。
 - 自动导入阿里云资产
 - 在自动导入阿里云资产提示对话框中，单击确认，直接导入当前阿里云账号下的ECS、SLB、EIP资产信息。
 - 若您在此处单击取消，后续您仍可以在设置页面，修改资产导入设置。

 说明 已勾选同意阿里云漏洞扫描系统关联您UID下的ECS、SLB、EIP资产信息后，则资产导入设置不可更改。

- 手动添加资产

- a. 在扫描目标页面，单击添加资产。

- b. 在添加资产侧边页，完成以下配置。

- 资产：输入要添加的主机IP或域名。支持添加多个资产，多个资产间以换行符分隔。
- 资产标签：从已有标签中选择一个标签，或者直接输入新标签，按回车键确认。

- c. 单击添加。

执行结果

成功添加的资产出现在扫描目标页面的资产列表中。

您可以单击切换域名和主机IP页签，分别查看已添加的域名和IP资产；也可以通过资产标签定位到具体资产。

后续步骤

[创建扫描任务](#)。

2.2. 管理资产

您可以管理已添加到漏洞扫描系统中的资产，具体包括管理标签（添加或移除标签）、删除资产。

前提条件

已添加资产。具体操作请参见[添加资产](#)。

操作步骤

1. 登录[漏洞扫描系统控制台](#)。
2. 在左侧导航栏，单击扫描目标。
3. 在所有资产列表中，定位到要操作的资产，根据需要执行以下操作。
 - 管理标签

- a. 您可以单击目标资产操作列下的标签单个管理资产标签，或勾选多个目标资产，单击资产列表下方的添加标签，批量管理资产标签。



- b. 在添加标签侧边页，添加或移除资产标签。

单个管理标签

批量管理标签

- c. 单击添加。


 说明 关于移除标签，具体操作可参见[标签分组](#)中的移除错误标签和删除标签。

- 删除资产
 - a. 您可以单击目标资产操作列下的删除单个删除资产。



- b. 在提示对话框中，单击确定。



 说明 您也可以勾选多个资产，单击资产列表下方的删除资产，同时删除多个资产。批量操作不会有提示框确认，会直接删除勾选中的资产，所以请谨慎操作。

2.3. 搜索资产

您可以对资产进行搜索，支持对域名和IP两种不同类型资产的搜索。

操作步骤

1. 登录[漏洞扫描系统控制台](#)。
2. 在左侧导航栏，单击扫描目标。
3. 您可以参考以下步骤搜索资产。

- 根据域名进行搜索：支持单域名和根域名两种检索方式。
 - 根据单域名检索：在搜索框中输入完整的域名，单击搜索按钮，界面显示该域名的资产信息。
□
 - 根据根域名检索：在搜索框中输入根域名，单击搜索按钮，界面显示该根域名下对应的子域名的资产信息。
□
- 根据IP进行搜索：支持单IP和CIDR段两种方式的检索。
 - 根据单IP检索：在搜索框中输入一个完整的IP地址，单击搜索按钮，界面显示该IP的资产信息。
□
 - 根据CIDR段检索：在搜索框中输入一个CIDR段地址，单击搜索按钮，界面显示该CIDR段下的资产信息。
□

2.4. 资产助手

您可以在资产助手中确认或删除关联出来的资产。

背景信息

当您为资产开通漏洞扫描服务后，系统默认会启动一个资产发现助手任务，基于自动导入的云上资产和用户所添加的资产，利用数据中的资产关联发现模型，进行周期性的资产关联发现，并同步到扫描目标 > 资产助手中。

② 说明 目前资产发现助手任务，运行周期为每7天一次。

操作步骤

1. 登录[漏洞扫描系统控制台](#)。
2. 在左侧导航栏，单击扫描目标 > 资产助手，可以查看资产助手关联到的资产信息。



3. 您可以在资产助手列表，确认或删除关联的资产。
 - 确认：此操作后，资产会进入到无标签资产列表中。

② 说明 您也可以在没有标签资产列表删除不需要检测的资产。

- 删除：此操作后，删除不需要漏洞检测的资产，从扫描资产列表中移除。



2.5. 标签分组

本文介绍漏洞扫描系统中资产标签分组管理功能。

背景信息

漏洞扫描系统支持标签形式来管理用户的资产，支持多对多形式对资产添加标签，便于您对不同的业务检测资产风险，更合理的管理业务资产。

操作步骤

1. 登录**漏洞扫描系统控制台**。
2. 在左侧导航栏，单击**扫描目标**。
3. 您可以执行以下步骤管理资产标签。

- 为“新增的资产”添加标签：在扫描目标页面，单击所有资产 > 添加资产，进入添加资产页面，为资产添加标签。




- 为“无标签资产”添加标签：在扫描目标页面，单击无标签资产，对无标签资产列表中的资产进行单个或批量添加标签。

完成添加标签后，资产将会从无标签资产列表中移除，进入对应的标签资产列表中。



- 移除错误标签：在扫描目标页面，单击扫描标签下的标签项，单击标记错误的资产右侧操作列下的移除标签，删除资产的标签，然后为资产添加正确的标签。

您也可以勾选标签下多个资产，单击资产列表下方的移除标签，同时为标签错误的多个资产移除标签。

 **说明** 移除标签后，该资产从标签列表中移除。如果勾选了标签下的所有资产，移除标签后，会直接删除此标签。



- 删除标签：在扫描目标页面，单击扫描标签下的标签项，全选所有资产，单击移除标签，移除所有资产，即可删除标签。



3. 扫描任务

3.1. 限制条件

使用阿里云漏洞扫描系统创建扫描任务前，请查看可用配额，以避免不必要的点数消耗。

您可在漏洞扫描系统控制台概览页面右侧可用配额下拉列表中查看您当前账号的可用配额和全部配额点数。



 **说明** 可用配额数量为0时将无法再进行扫描，单击增加配额重新购买站点数。详细信息参见[升级和续费](#)。

3.2. 创建扫描任务


阿里云漏洞扫描支持创建扫描任务，您可以创建资产发现和漏洞扫描两种不同扫描策略的扫描任务。当您网站资产成功添加为漏洞扫描系统的扫描目标后，您可以为其创建扫描任务。本文介绍了创建扫描任务的具体操作。

前提条件

已添加资产。具体操作请参见[添加资产](#)。

背景信息

- 创建扫描任务时，单个扫描任务支持的扫描对象包括：
 - 单个或多个指定资产
 - 单个或多个指定标签下的所有资产
- 在为多个资产配置扫描任务时，推荐您使用资产标签，先为要操作的资产添加一个相同的标签，然后以标签作为扫描对象创建扫描任务。关于如何批量设置标签，请参见[管理资产](#)。
- 创建扫描任务时，支持选择创建资产发现或漏洞扫描两种不同扫描策略的任务。
 - 资产发现**：检测发现指定资产在公网上的域名、IP、端口、URL或服务等信息。
 - 漏洞扫描**：检测指定资产或URL上存在的漏洞和风险。
- 创建扫描任务时，支持选择创建单次执行任务、定期执行任务，或者周期执行任务。

 **说明** 在创建扫描任务前，请查看可用配额，以避免不必要的点数消耗。具体内容，请参见[限制条件](#)。

操作步骤

- 登录[漏洞扫描系统控制台](#)。
- 在左侧导航栏单击任务管理 > 扫描目标。
- 根据您的需要，从以下方式中选择合适的方式，添加扫描对象。
 - 扫描指定单个或多个资产**：在资产列表中勾选要扫描的网站资产，单击已选中资产（任意一个）操作列的扫描，打开创建扫描任务侧页面。



- **扫描指定资产组中所有资产**：直接单击资产列表上方的**扫描**。打开创建扫描任务侧页面，其中扫描目标配置支持从已有标签中进行选择。



4. 完成扫描任务的配置（见下表）。

配置	描述
任务名称	系统会自动匹配一个任务名称，支持自定义，建议输入便于识别的名称。
扫描目标	指定要扫描的资产对象。可以手动输入域名或IP，或从下拉框中选择一个或多个资产标签。
扫描策略	指定执行扫描任务的策略。可选漏洞扫描或资产发现。
允许扫描时间段	<p>设置允许启用扫描任务的时间段。扫描任务只会在您设置的允许时间段内执行。</p> <div style="border: 1px solid #ccc; background-color: #e0f2f1; padding: 5px; margin-top: 5px;"> ? 说明 建议您设置在非业务高峰期允许扫描。 </div>
扫描计划	<p>设置扫描任务的执行方式，取值：</p> <ul style="list-style-type: none"> ○ 立即开始：创建完任务后，在最近的允许扫描时间段内执行扫描。 ○ 定时启动：创建完任务后，在指定的启动时间后，且在允许扫描时间段执行扫描。 ○ 周期任务：任务启动后，以指定的频率（每天、每周、每月）并在指定的启动时间后，且在允许扫描时间段执行扫描。
启动时间	扫描计划为定时启动或者周期任务时，设置任务启动时间。扫描任务将在设置的启动时间后，且在允许扫描时间段启动。
实例创建周期	<p>扫描计划为周期任务时，设置任务的执行频率。取值：</p> <ul style="list-style-type: none"> ○ 每天 ○ 每周 ○ 每月 <p>扫描任务启动后，将按照指定的频率周期执行。</p>

5. 单击创建。

执行结果

成功创建的扫描任务出现在扫描任务列表中。



后续步骤

[管理扫描任务。](#)

3.3. 管理扫描任务

完成扫描任务创建后，您可以管理扫描任务和周期计划。

前提条件

已创建扫描任务。具体操作请参见[创建扫描任务](#)。

管理任务和周期

您可以执行以下步骤管理扫描任务和周期计划。

1. 登录[漏洞扫描系统控制台](#)。
2. 在左侧导航栏，单击**扫描任务**，根据需要执行以下操作。

- **查看和搜索任务**

- **查看任务**



- **搜索任务**

您可以在搜索框，输入需要查找的IP/域名/任务名，定位对应的任务列表，后台会根据创建时间进行排序并返回结果至列表。



- **筛选任务**

目前可以支持根据任务调度周期类型，对任务列表进行筛选，您可以根据所关注的调度周期类型（**单次任务、周期任务**）进行筛选。而默认全部情况，任务列表会按照创建时间来进行排序。

- **筛选单次任务**，关注立即执行和定时启动的任务列表。



- **筛选周期任务**，关注所创建调度周期为**每天、每周、每月**的任务列表。



- **编辑和删除任务**

- **编辑任务**

- a. 您可以单击任务列表里的操作列的编辑，对任务进行编辑。



- b. 您可以在展开的编辑扫描任务侧页面，对任务选项进行编辑修改。

目前支持可编辑的参数项有**任务名称、允许扫描时间段、启动时间（立即启动及定时启动）和扫描周期（每天、每周、每月）**。任务创建后，暂不支持修改扫描计划。



- c. 单击确定。

- **删除任务**

您可以单击任务列表里操作列的删除，对选定的任务进行删除。漏洞扫描系统支持批量删除扫描任务。



○ 查看任务实例列表

- 您可以在任务列表页面，单击任务名称/扫描目标或任务实例列（运行中/已完成/已停止|全部状态），进入并查看对应任务的任务实例列表。



- 您还可以根据状态筛选栏，筛选不同状态类型的任务。支持多种实例状态（等待中、运行中、已停止、已完成、暂停中）的筛选。



○ 开启和关闭周期任务

用户可以在启用状态列，对周期任务的调度状态进行开启/关闭操作，调度引擎会根据此状态来决定是否调度，创建新的任务实例来进行扫描。



3.4. 管理任务实例

完成扫描任务创建后，您可以管理任务实例和漏洞风险。

前提条件

已创建扫描任务。具体操作请参见[创建扫描任务](#)。

操作步骤

1. 登录[漏洞扫描系统控制台](#)。
2. 在左侧导航栏，单击任务实例，根据需要执行以下操作。

○ 查看/搜索/筛选任务实例

- 您可以在任务实例列表页面，看到当前根据扫描任务，所创建的任务实例列表及对应相关信息。



其中，漏洞数列显示不同危害等级的漏洞数量。关于漏洞危害等级的定义，请参见下表描述。

等级	描述
高危	可以直接被利用的漏洞，且利用难度较低。被攻击之后可能对网站或服务器的正常运行造成严重影响，或对用户财产及个人信息造成重大损失。
中危	被利用之后，造成的影响较大，但直接利用难度较高的漏洞。或本身无法直接攻击，但能为进一步攻击造成便利的漏洞。
地危	无法直接实现攻击，但提供的信息可能让攻击者更容易找到其他安全漏洞。
信息	本身对网站安全没有直接影响，提供的信息可能为攻击者提供少量帮助，或可用于其他手段的攻击，如社工等。

- 您可以根据需求，在搜索栏，输入IP/域名/任务名，定位到对应任务实例。显示的列表信息会根据扫描开始时间，对任务实例进行排序。



- 您还可以根据状态筛选栏，筛选不同状态类型的任务。支持多种实例状态（等待中、运行中、已停止、已完成、暂停中）的筛选；支持与搜索栏IP/域名/任务名叠加检索。



- 查看任务实例详情

- a. 您可以在任务实例列表页，单击实例名称/扫描目标，进入任务实例详情页。



- b. 您可以在任务实例详情页面，查看任务实例详细运行数据。

- 实例概览：包含任务实例运行概要信息，任务状态信息，及风险统计信息。
- 攻击面：主要包含任务实例对资产进行扫描的攻击面数据项（域名、子域名、端口服务、Web应用等）。
- 风险概况：主要包含任务实例运行所发现的风险聚合信息。



- 查看和导出攻击面数据详情

您可以从任务实例详情的攻击面部分进入数据项的详情页面。数据项包含以下几种：域名、子域名、DNS解析记录、主机列表、端口服务、Web应用、Web服务器、Web路径、爬虫流量。

单击相应数据项详情按钮，进入对应数据详情页，了解攻击面数据详情。



- 域名攻击面数据



- 子域名攻击面数据



- 端口服务攻击面数据

您可以查看对应主机开放的端口服务详情。



- Web应用攻击面数据

您可以查看对应站点的Web应用（CMS/Framework 等）的数据。



- 其他数据项

您可以参照以上示例查看其他数据项攻击面数据。

■ 导出攻击面数据

您可以导出CVS格式的攻击面数据列表。

- a. 单击对应数据项攻击面数据详情列表右上角导出，界面显示导出中。



- b. 然后刷新页面，可以查看最新导出状态。当后端导出任务完成时，界面显示下载，单击下载导出数据。



已导出CSV 格式数据示例如下，您可以导入自己的数据系统，进行相应分析。



○ 查看风险资产详情

- 您可以从任务实例详情页面，进入风险资产列表，并进入风险资产详情页面。

风险概况从域名/IP维度，对包含风险的资产，进行全面审计，帮助您进行更细粒度的风险管理。



- 您可以在风险资产列表侧边栏，单击主机（IP）项，进入风险主机详情页，查看风险主机详情。

在风险主机详情页面，包含主机和攻击面数据项（Web 路径、端口服务、爬虫流量、Web 应用）相关数据。



- 您可以在风险资产列表侧边栏，单击域名（Domain）项，进入风险域名详情页，查看风险域名详情。



在风险域名详情页面，包含域名相关详情，和攻击面数据项（Web 路径、Web 服务器、爬虫流量、Web 应用）相关数据。



○ 查看漏洞详情页

您可以从任务实例详情页和风险资产（主机/域名）详情页，两个维度进入漏洞详情页，对相关漏洞风险进行审核处理。

- 实例详情维度

- a. 在任务实例详情页，风险概况部分，单击任意漏洞名称，进入漏洞详情侧页面。



- b. 在漏洞详情页，会显示这个任务实例维度下，该漏洞类型漏洞条目聚合的结果，及对应处理状态。



- c. 单击左侧的展开按键，会显示漏洞条目的具体漏洞证明详情。您可以依次进行漏洞验证和复现。

19



- **风险资产维度：**同任务实例详情页操作类似，单击任意漏洞名称，即进入漏洞详情侧页面。

该页面会聚合在此任务实例下资产的漏洞详情，更进一步细粒度聚合，帮助您提升漏洞处理效率。



- **任务检测项详情**

- a. 您可以在任务实例详情页，单击实例概览 > 实例信息 > 检测项，进入检测项详情页，查看对应任务实例的检测步骤详情。



- b. 在检测项详情页，主要包含整个任务实例运行的所有检测项。您可以通过该页面查询所关注的检测项（如 Redis、Hadoop、MongoDB 等中间件）类型，及对应检测项是否包含风险等。



- **安全评估报告**

您可以生成并下载安全评估报告至本地，便于本地查看分析。

- a. 您可以在任务实例页面，单击报表栏下的生成，生成任务实例对应的安全评估报告。



- b. 报告生成完成后，单击下载。



- c. 解压下载的安全评估报告ZIP包，打开 *index.html* 文件，即可浏览报告详情。



4.攻击面透视

4.1. 概述

攻击面透视功能为您提供基于域名、端口、主机列表及Web应用列表等不同类型攻击面数据的查询管理功能，帮助您提升资产攻击面数据的管理效率。

攻击面透视模块支持查询以下类型的攻击面数据：

- 域名
- 子域名
- 主机列表
- DNS解析记录
- 端口服务
- Web应用
- Web路径

4.2. 攻击面数据查询

攻击面透视服务提供一套查询语法用于设置查询条件，帮助您方便快捷地查询攻击面数据。

查看攻击面概览数据

1. 登录[漏洞扫描系统控制台](#)。
2. 在左侧导航栏单击概览。
3. 在概览页面定位到资产攻击面模块，查看您资产的攻击面相关的全方位概览信息。



查询攻击面数据

1. 登录[漏洞扫描系统控制台](#)。
2. 在左侧导航栏单击实验室 > 攻击面透视。
3. 在攻击面透视页面中单击需要查询的数据源（攻击面类型）页签。

攻击面透视模块支持查询以下类型的攻击面数据：

- 域名
 - 子域名
 - 主机列表
 - DNS解析记录
 - 端口服务
 - Web应用
 - Web路径
4. 在攻击面数据源页签中通过搜索查询该数据源中的攻击面信息，包括漏洞扫描检测到的攻击面数据的更新时间、可执行的操作等。您可以通过以下两种方式查询攻击面数据。
 - 模糊查询

您可以在数据源页签的搜索栏中直接输入查询的关键字，漏洞扫描会根据不同的数据源模糊检索每个数据源对应的相关字段，并为您展示相应的查询结果。

例如：在子域名页签的搜索栏中，输入 *aliyun* 或者 *aliyun.com* 都可以查询到 *aliyun.com* 相关的子域名和根域名信息，以及该子域名执行过的漏洞扫描的概览信息。

○ 字段查询

您可以在数据源页签的搜索栏中直接输入查询字段 `<字段名>:<查询内容>`，即可检索到相应的查询结果。

说明 查询字段中的 `:` 需使用半角符号。其他查询语句说明和示例请参见 [字段查询运算符](#) 和 [查询字段与示例](#)。

例如：在端口服务页签的搜索栏中，输入 `ip:1.2.3.4`，表示查询IP地址为 `1.2.3.4` 的服务器上开启的服务端口。

输入字段查询攻击面数据后，单击 **另存为标签** 并在 **另存为标签** 页面中输入自定义的标签名称，将该检索的字段保存为资产标签，方便您在 **创建扫描任务** 时直接选中该资产标签作为扫描目标。

4.3. 字段查询运算符

攻击面透视功能支持使用查询语法来查询相关信息。本文档列举了攻击面透视字段查询需要使用到的运算符。

字段查询支持的运算符

运算符	说明	附加说明
AND	格式为 <code>query1 AND query2</code> ，表示“与”关系，同时满足 <code>query1</code> 与 <code>query2</code> 两个条件的查询结果。	多个查询条件关键词之间如果没有使用运算符链接，默认是 <code>AND</code> 的关系。
OR	格式为 <code>query1 OR query2</code> ，表示“或”关系，同时满足 <code>query1</code> 或 <code>query2</code> 两个条件的查询结果。	-
NOT	格式为 <code>NOT query1</code> ，表示“非”关系，即排除 <code>query1</code> 的查询结果。可与 <code>AND</code> 和 <code>OR</code> 一起连用。	-
""	格式为 <code><field>:"query1"</code> ，表示精确匹配，即满足字段内容精确为 <code>query1</code> 的查询结果。	-


运算符	说明	附加说明
>	查询某个字段中大于某个数值的结果。目前仅支持端口服务的 <i>port</i> 字段查询。例如： <i>port > 80</i> 即查询端口大于80的结果。	-
>=	查询某个字段中大于等于某个数值的结果。目前仅支持端口服务的 <i>port</i> 字段查询。例如： <i>port >= 80</i> 即查询端口大于等于80的结果。	-
<	查询某个字段中小于某个数值的结果。目前仅支持端口服务的 <i>port</i> 字段查询。例如： <i>port < 8080</i> 即查询端口小于8080的结果。	-
<=	查询某个字段中小于等于某个数值的结果。目前仅支持端口服务的 <i>port</i> 字段查询。例如： <i>port <= 8080</i> 即查询端口小于等于8080的结果。	-

4.4. 查询字段与示例

本文档列举了在漏洞扫描控制台攻击面透视页面中对各个数据源进行查询的字段和示例，您可以参考本文档提供的示例了解如何快速查询不同数据源的攻击面信息。

背景信息

有关攻击面数据查询的详细操作请参见[攻击面数据查询](#)。

 **说明** 查询具体端口、解析地址、子域名时，查询字段中必须使用半角双引号 (") 进行精确匹配查询，避免出现语句符号冲突导致查询失败。详细字段结构请参见下表中具体的查询语句示例。

域名查询

在攻击面透视 > 域名页面搜索框中输入关键词 *aliyun* 进行搜索，可以检索到 *aliyun* 相关的域名。

子域名查询

查询子域名支持使用的字段如下所示。

字段	说明	查询语句示例
domain	查询根域名。	<i>domain:aliyun.com</i>
subdomain	查询子域名。	<i>subdomain:aliyun.com, subdomain:"1.aliyun.com"</i>

例如：在攻击面透视 > 子域名页面搜索框中输入字段 `domain:aliyun.com`（根域名查询字段）或者 `subdomain:aliyun.com`（子域名查询字段）进行搜索，可以检索到 `aliyun` 相关的根域名或子域名信息。

主机列表

查询主机列表支持使用的字段如下所示。

字段	说明	查询语句示例
ip	查询具体IP地址对应的主机信息。	<code>ip:1.2.3.4</code>
cidr	查询CIDR地址对应的主机信息。	<code>cidr:1.2.3.4/24</code>
hostname	查询主机名对应的主机列表信息。	<code>hostname:guest</code>
state	查询主机状态。	<ul style="list-style-type: none"> 输入 <code>state:up</code> 可以查询状态为在线的主机。 输入 <code>state:down</code> 可以查询状态为离线的主机。
os	查询安装了某类操作系统的主机的列表信息。	<code>os:windows</code>

例如：在攻击面透视 > 主机列表页面搜索框中输入字段 `cidr:192.168.1.1/24 os:linux state:up` 查询 `192.168.1.1/24` 地址段下在线状态的Linux主机。

DNS解析记录

查询DNS解析记录支持使用的字段如下所示。

字段	说明	查询语句示例
domain	查询某个根域名的DNS解析记录。	<code>domain:aliyun.com</code>
subdomain	查询某个子域名的DNS解析记录。	<code>subdomain:1.aliyun.com</code>
record	查询某个解析记录的列表信息。	<code>record:"1.2.3.4"</code>
type	查询某个解析记录类型的解析记录列表信息。	<ul style="list-style-type: none"> 输入 <code>type:a</code> 查询解析记录类型为 <code>a</code> 的解析记录列表。 输入 <code>type:cname</code> 查询解析记录类型为 <code>cname</code> 的解析记录列表。

例如：在攻击面透视 > DNS解析记录页面搜索框中输入字段 `domain:aliyun.com type:a`，查询域名 `aliyun.com` 解析记录类型为A的DNS解析记录列表。

端口服务

查询端口服务支持使用的字段如下所示。

字段	说明	查询语句示例
ip	查询某个IP地址的主机列表信息。	<i>ip:1.2.3.4</i>
icdr	查询某个CIDR地址段中所有的IP地址对应的主机列表信息。	<i>cidr:1.2.3.4/24</i>
port	查询开启了某个端口的主机的列表信息。	<i>port:80</i>
protocol	查询端口支持的某类协议的列表信息。支持TCP和UDP协议。	<i>protocol:tcp</i>
service	查询支持某类端口服务的列表信息。支持的端口服务包括HTTP、HTTPS、HTTP-PROXY、MS-WBT-Server、SSH等。	<i>service:http</i>
product	查询某个产品的列表信息。支持的产品（提供端口服务的应用或设备）包括：Apache、Nginx等。您可以在端口服务页面查看支持的所有产品名称。	<i>product:apache</i>
version	查询某个产品版本号对应的列表信息。	<i>version:1.0.2</i>

例如：在攻击面透视 > 端口服务页面搜索框中输入字段 *port:80 product:nginx* 查询开放的端口号为80的Nginx主机列表。输入字段 *cidr:1.2.3.4/24 service:http* 查询 `1.2.3.4/24` 这个地址段下所有IP地址对应的主机的http服务。

Web应用

查询Web应用支持使用的字段如下所示。

字段	说明	查询语句示例
domain	查询某个域名下使用的Web应用列表信息。	<i>domain:aliyun.com</i>
name	查询使用了某个应用的站点列表信息。	<i>name:wordpress</i>
title	使用标题名称关键词查询站点的列表信息。	<i>title:console</i>
server	查询使用了某个服务器类型的站点列表信息。	<i>server:apache</i>
version	查询应用了某个版本号的站点列表信息。	<i>version:1.2.0</i>

例如：在攻击面透视 > Web应用页面搜索框中输入字段 *domain:aliyun.com name:wordpress* 查询 *aliyun.com* 域名中WordPress相关的站点列表。

Web路径

查询Web应用支持使用的字段如下所示。

字段	说明	查询语句示例
hostname	查询某个域名下的站点和Web路径信息。	<i>hostname:aliyun.com</i>
netloc	查询某个域名下端口提供的同一个应用服务对应的站点信息。	<i>netloc:"www.aliyun.com:81"</i>

例如：在攻击面透视 > Web路径页面搜索框中输入字段 *hostname:abc.com* 查询 *abc.com* 域名下的Web路径信息列表。

5. 风险

您可以在漏洞扫描系统的风险页面查看检测发现的漏洞和内容风险详情并进行处理。

操作步骤

1. 登录[漏洞扫描系统控制台](#)。
2. 在左侧导航栏，单击[风险](#)。
3. 在风险列表页面，您可以查看和管理漏洞和内容风险，根据需要执行以下操作。

○ 查看和搜索漏洞

在漏洞页，可以通过风险状态（已处理、未处理、误报、白名单）、威胁程度（高危、中危、低危、信息）、漏洞类型、资产域名或IP和发现时间中任意项搜索定位到资产漏洞信息。



○ 查看漏洞详情

您可以单击漏洞名称，查看漏洞详情，包括漏洞描述、漏洞证明、漏洞造成的影响、安全建议和技术参考。



○ 管理漏洞

执行下表中相应操作管理资产漏洞。



操作	描述
设为已处理	当已确认和修复对应漏洞时，可执行此操作，漏洞状态变为已处理。
加入白名单	当不再需要检测一个漏洞时，可执行此操作，系统不再检测对应漏洞，漏洞状态变为白名单。
标记为误报	当确认不存在对应漏洞时，可执行此操作，漏洞状态变为误报。

- **单个管理**：您可以在漏洞页，单击单个漏洞右侧操作列的相应操作，或在一个漏洞详情页，单击相应操作，管理资产漏洞。
- **批量管理**：您可以在漏洞页，勾选多个漏洞，单击漏洞列表下方的相应操作管理资产漏洞。

○ 查看和搜索内容风险

- 在内容风险页，可以通过风险状态（已处理、未处理、误报、白名单）、威胁程度（高危、中危、低危、信息）、资产域名或IP和发现时间中任意项搜索定位到资产内容风险信息。



- 在内容风险页的风险列表中，定位到目标风险项并单击风险名称下的源码风险图标或文本风险图标查看对应的源码和文本风险内容。



○ 管理风险内容

执行下表中相应操作管理检测的风险内容。

操作	描述
设为已处理	当已确认并处理风险内容时，可执行此操作，风险状态变为已处理。
加入白名单	当不再需要检测一个风险内容时，可执行此操作，系统不再检测对应风险内容，风险状态变为白名单。
标记为误报	当确认不存在对应风险内容时，可执行此操作，风险状态变为误报。

- **单个管理：**您可以在风险内容页，单击单个风险右侧操作列的相应操作管理资产风险内容。
- **批量管理：**您可以在风险内容页，勾选多个风险，单击风险列表下方的相应操作管理资产风险内容。