

# Alibaba Cloud

## 漏洞扫描

### 快速入门

文档版本：20200113

# 法律声明

---

阿里云提醒您在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。	 <b>禁止：</b> 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。	 <b>警告：</b> 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。	 <b>注意：</b> 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。	 <b>说明：</b> 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。
<b>粗体</b>	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 <code>cd /d C:/window</code> 命令，进入Windows系统文件夹。
##	表示参数、变量。	<code>bae log list --instanceid Instance_ID</code>
[ ]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

---

法律声明.....	I
通用约定.....	I
1 限制说明.....	1
2 快速入门.....	2

# 1 限制说明

---

漏洞扫描的限制说明。

漏洞扫描包含以下使用限制：

- 不得基于漏洞扫描或其内容进行修改、制作、派生衍生作品/产品，不得复制和模仿漏洞扫描的设计理念、界面、功能和图表，不得将漏洞扫描的使用转让、出借、出租、再许可或用于任何商业目的。
- 不得对漏洞扫描和/或其任何部分（包括页面标识、服务品牌、资讯、数据等）进行复制、翻译、修改、反编译、反汇编、反向工程、分解拆卸，不修改或拆分漏洞扫描的代码或者任何功能。
- 您利用漏洞扫描进行漏洞扫描的业务须为正常的商业、科研等符合国家法律规定的业务，不得用于从事任何非法业务。
- 您使用漏洞扫描进行漏洞扫描的业务必须为自有业务，不得利用漏洞扫描对其他任何第三方的网站、服务器或业务进行漏洞扫描；若用户违反该约定的，阿里云有权立即终止您对如漏洞扫描的使用，且造成的阿里云及任何第三方的全部损失均由用户承担。
- 不进行任何破坏或试图破坏网络安全的行为（包括但不限于钓鱼、黑客、网络诈骗、网站或空间中含有或涉嫌散播：病毒、木马、恶意代码，及通过虚拟服务器对其他网站、服务器进行涉嫌攻击行为如扫描、嗅探、ARP欺骗、DDoS等）。
- 不进行任何改变或试图改变阿里云提供的系统配置或破坏系统安全的行为。不利用阿里云提供的服务从事损害阿里云及阿里云关联公司、任何第三方的合法权益的行为。
- 不从事其他违法、违规或违反阿里云服务条款的行为。

## 2 快速入门

本文介绍了使用云盾漏洞扫描系统对您的网站资产进行漏洞扫描的操作流程，具体包括添加资产、创建扫描任务、查看扫描结果。

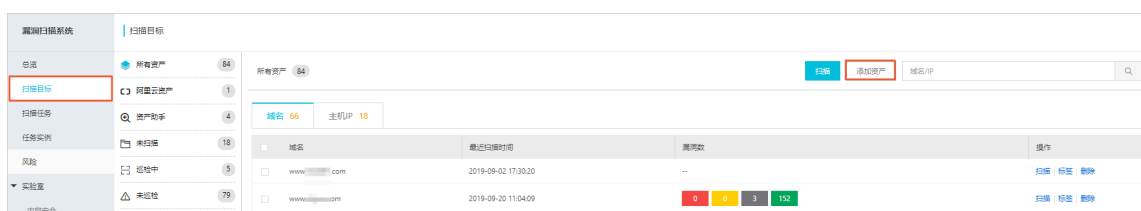
### 前提条件

如果您已经为网站资产部署了Web应用防火墙（WAF）或安全运营中心（SOC）等安全防护监控系统，请务必将云盾漏洞扫描的扫描引擎IP段添加至WAF或SOC产品的白名单中，确保漏洞扫描任务可正常运行。

关于云盾漏洞扫描的扫描IP段，查看[漏洞扫描常见问题](#)。

### 操作步骤

1. 登录[云盾漏洞扫描管理控制台](#)。
2. 在左侧导航栏，单击扫描目标进入资产页面。
3. 添加资产
  - a. 在扫描目标页面，单击添加资产。



#### 说明:

阿里云资产支持自动关联，具体请参见[#unique\\_6](#)。

- b. 在添加资产侧边页，填写所需检测的资产。



- c. 下拉资产标签，选择或创建所需标签（例如，靶场），资产将归属到所选择的标签下。



#### 说明:

当您所需的标签不存在时，可以按回车创建标签。

添加资产

资产: 请输入IP或域名，以换行分割

资产标签: 靶场

添加 取消

d. 单击添加。

成功添加资产后，您可以在对应标签下看到已添加资产。

漏洞扫描系统 | 扫描目标

所有资产 84

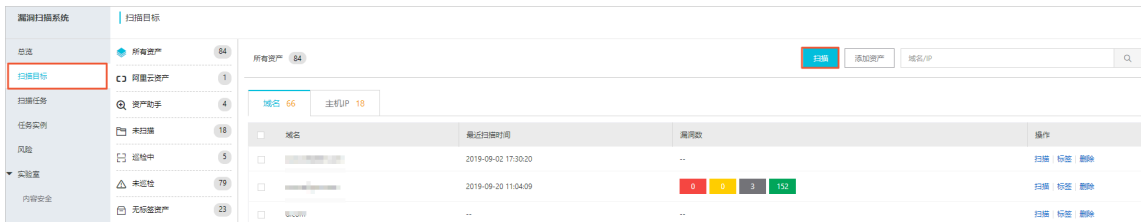
资产 4

IP	最后扫描时间	漏洞数	操作
10.10.10.10	2019-09-20 11:04:09	65 379 288 146	扫描 标签 移除标签

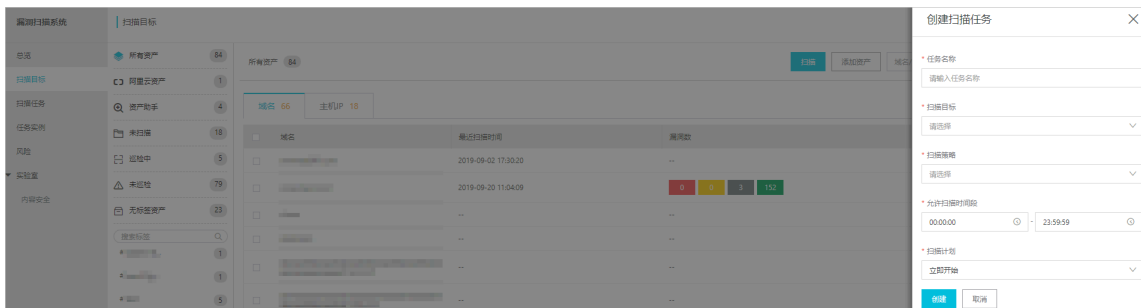
共有 1 条 < 上一页 1 下一页 >

### 4. 快速创建扫描任务


a. 在扫描目标页面，单击资产列表上方的扫描，打开创建扫描任务侧边页。



b. 在创建扫描任务侧边页，根据需要完成任务配置。

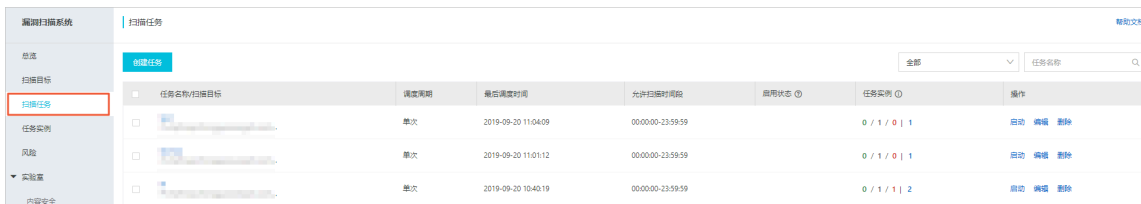



- 扫描目标：支持从已有标签中选择，系统将扫描选中标签下的所有资产。
- 允许扫描时间段：规定了允许漏洞扫描系统在您的资产上进行扫描的时间范围。
- 扫描计划：支持立即开始、定时启动、周期任务三种模式。

 **说明：**  
关于具体的任务配置说明，请参见[#unique\\_7](#)。

c. 单击创建。

成功创建扫描任务后，漏洞扫描系统为该任务生成一个任务实例，您可以在扫描任务页面，看到已创建的扫描任务，并通过输入任务名/IP/域名搜索定位到具体的任务实例。



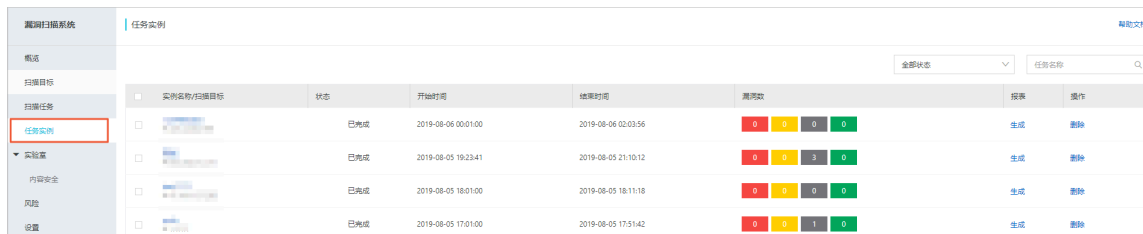
 **说明：**  
任务名/IP/域名支持模糊搜索。



## 5. 查看任务实例详情

等待扫描任务启动并执行完成后，前往任务实例页面，查看扫描任务的任务详情及扫描结果。

a. 在左侧导航栏，单击任务实例进入任务实例页面，查看实例列表信息。



实例名称/扫描目标	状态	开始时间	结束时间	高危数	中危数	低危数	信息数	报表	操作
...	已完成	2019-08-06 00:01:00	2019-08-06 02:03:56	0	0	0	0	生成	删除
...	已完成	2019-08-05 19:23:41	2019-08-05 21:10:12	0	0	3	0	生成	删除
...	已完成	2019-08-05 18:01:00	2019-08-05 18:11:18	0	0	0	0	生成	删除
...	已完成	2019-08-05 17:01:00	2019-08-05 17:51:42	0	0	1	0	生成	删除

b. 单击任务的实例名称/扫描目标，进入任务实例详情页，查看任务实例详情数据。



### 说明:

您也可以通过任务实例列表中报表操作，生成并下载安全评估报告。具体操作请参见#unique\_8中的管理任务实例。