天翼云·漏洞扫描（专业版）

用户使用指南

天翼云科技有限公司

目 录

1 产品简介

1.1 漏洞扫描服务

漏洞扫描服务（Vulnerability Scan Service，简称 VSS）是针对网站、主机进行漏洞扫描的一种安全检测服务，目前提供通用漏洞检测、漏洞生命周期管理服务。

工作原理

漏洞扫描服务具有 Web 网站扫描和主机扫描两种扫描能力。

- Web 网站扫描

  采用网页爬虫的方式全面深入的爬取网站 url，基于多种不同能力的漏洞扫描插件，模拟用户真实浏览场景，逐个深度分析网站细节，帮助用户发现网站潜在的安全隐患。同时内置了丰富的无害化扫描规则，以及扫描速率动态调整能力，可有效避免用户网站业务受到影响。

- 主机扫描

  经过用户授权（支持账密授权）访问用户主机，漏洞扫描服务能够自动发现并检测主机操作系统、中间件等版本漏洞信息和基线配置，实时同步官网更新的漏洞库匹配漏洞特征，帮助用户及时发现主机安全隐患。

1.2 功能特性

漏洞扫描服务可以帮助您快速检测出您的网站、主机存在的漏洞，提供详细的漏洞分析报告，并针对不同类型的漏洞提供专业可靠的修复建议。

- 网站漏洞扫描
  - 具有 OWASP TOP10 和 WASC 的漏洞检测能力，支持扫描 22 种类型以上的漏洞。
  - 扫描规则云端自动更新，全网生效，及时涵盖最新爆发的漏洞。
  - 支持 HTTPS 扫描。
- 一站式漏洞管理

  - 提供漏洞修复建议。如果您需要查看修复建议，请购买专业版、高级版或者企业版。
  - 支持下载扫描报告，用户可以离线查看漏洞信息。如果您需要下载扫描报告，请购买专业版、高级版或者企业版。
  - 支持重新扫描。
- 支持弱密码扫描
  - 多场景可用

    支持操作系统(RDP 协议、SSH 协议)、数据库（如 Mysql、Redis）等常见中间件弱口令检测。
  - 丰富的弱密码库

    丰富的弱密码匹配库，模拟黑客对各场景进行弱口令探测。
- 支持端口扫描

  扫描服务器端口的开放状态，检测出容易被黑客发现的“入侵通道”。
- 自定义扫描
  - 支持任务定时扫描。
  - 支持基于用户名密码登录、基于自定义 Cookie 登录。
  - 支持 Web 2.0 高级爬虫扫描。
  - 支持自定义 Header 扫描。
  - 支持手动导入探索文件来进行被动扫描。
- 主机漏洞扫描
  - 支持深入扫描

    通过配置验证信息，可连接到服务器进行 OS 检测，进行多维度的漏洞、配置检测。
  - 支持内网扫描

    可以通过跳板机方式访问业务所在的服务器，适配不同企业网络管理场景。
  - 支持中间件扫描
    - 丰富的扫描场景

      支持主流 Web 容器、前台开发框架、后台微服务技术栈的版本漏洞和配置合规扫描。
    - 多扫描方式可选

      支持通过标准包或者自定义安装等多种方式识别服务器的中间件及其版本，全方位发现服务器的漏洞风险。

1.3 产品优势

扫描全面

涵盖多种类型资产扫描，支持云内外网站、主机漏洞，智能关联各资产，自动发现资产指纹信息，避免扫描盲区。

简单易用

配置简单，一键全网扫描。可自定义扫描事件，分类管理资产安全，让运维工作更简单，风险状况更清晰了然。

高效准确

- 采用 Web2.0 智能爬虫技术，内部验证机制不断自测和优化，提高检测准确率。
- 时刻关注业界紧急 CVE 爆发漏洞情况，自动扫描，快速了解资产安全风险。

报告全面

清晰简洁的扫描报告，多角度分析资产安全风险，多元化数据呈现，将安全数据智能分析和整合，使安全现状清晰明了。

1.4 产品规格差异

漏洞扫描服务提供了基础版、专业版、高级版和企业版四种服务版本。其中，基础版配额内的服务免费，部分功能按需计费；专业版、高级版和企业版需要收费。

VSS 各服务版本支持的计费方式、功能和规格说明如下所示，您可以根据业务需求选择相应的服务版本。

表1-1 VSS 各服务版本计费方式

服务版本	支持的计费方式	说明
基础版	• 配额内的服务免费 • 按需计费	• 基础版配额内仅支持 Web 网站漏洞扫描（域名个数：5 个，扫描次数：5 个域名每日总共可以扫描 5 次）是免费的。 • 基础版提供的以下功能按需计费： 1. 可以将 Web 漏洞扫描或主机漏洞扫描任务升级为专业版规格进行扫描，扫描完成后进行一次性扣费。 2. 主机扫描一次最多支持 20 台主机。
专业版	包年/包月	相对于按需付费，包年/包月购买方式能够提供更大的折扣，对于长期使用者，推荐该方式。包周期计费为按照订单的购买周期来进行结算。
高级版	包年/包月	
企业版	包年/包月	

表1-2 VSS 各服务版本功能说明

功能	基础版	专业版	高级版	企业版
常见 Web 漏洞检测	√	√	√	√

功能	基础版	专业版	高级版	企业版
端口扫描	√	√	√	√
自定义登录方式	√	√	√	√
Web 2.0 高级爬虫	√	√	√	√
网站指纹识别	√	√	√	√
扫描任务管理	√	√	√	√
漏洞查看及管理	√	√	√	√
CVE 漏洞扫描	×	√	√	√
弱密码检测	×	√	√	√
网页内容合规检测（文字）	×	√	√	√
操作系统漏洞扫描	×	√	√	√
操作系统基线检查	×	√	√	√
中间件基线检查	×	√	√	√
查看漏洞修复建议	×	√	√	√
下载扫描报告	×	√	√	√
安全监测（定时扫描）	×	√	√	√
网页内容合规检测（图片）	×	×	×	√
网站挂马检测	×	×	×	√
链接健康检测（死链、暗链、恶意外链）	×	×	×	√
操作系统等保合规检查	×	×	×	√

表1-3 VSS 各服务版本支持的扫描配额说明

版本	域名/IP 个数	扫描次数	单个任务时长	任务优先级	单用户并发扫描数
基础版	Web 漏扫：包含 5 个二级域名或 IP:端口。	Web 漏扫：5 个域名每日总共可以扫描 5 次	2 小时	低	默认 Web 漏扫最大并发为 1 个域名。
专业版	Web 漏扫：包含 1 个二级域名或 IP:端口。		无限制	高	默认 Web 漏扫最大并发为 3

版本	域名/IP 个数	扫描次数	单个任务时长	任务优先级	单用户并发扫描数
	主机漏扫：包含 20 个 IP 地址。				个域名。 默认主机漏扫最大并发为 5 个 IP。
高级版	Web 漏扫：默认包含 1 个一级域名（不限制下属二级域名个数）/IP（不限制端口个数）。 主机漏扫：不限制 IP 地址个数。		无限制	高	默认 Web 漏扫最大并发为 5 个域名。 默认主机漏扫最大并发为 10 个 IP。
企业版	Web 漏扫：默认包含 5 个一级域名（不限制下属二级域名个数）/IP（不限制端口个数）。 主机漏扫：不限制 IP 地址个数。 说明 当默认的扫描配额不能满足您的需求时，您可以通过购买扫描配额包增加扫描配额（一个扫描配额包中包含一个一级域名扫描配额）。		无限制	高	默认 Web 漏扫最大并发为 10 个域名。 默认主机漏扫最大并发为 20 个 IP。 说明 更高并发需要，请提交工单联系专业工程师为您服务。

1.5 应用场景

漏洞扫描服务主要用于以下场景。

- Web 漏洞扫描应用场景

  网站的漏洞与弱点易于被黑客利用，形成攻击，带来不良影响，造成经济损失。

  - 常规漏洞扫描

    丰富的漏洞规则库，可针对各种类型的网站进行全面深入的漏洞扫描，提供专业全面的扫描报告。

  - 最新紧急漏洞扫描

    针对最新紧急爆发的 CVE 漏洞，安全专家第一时间分析漏洞、更新规则，提供快速专业的 CVE 漏洞扫描。

- 主机漏洞扫描应用场景

  运行重要业务的主机可能存在漏洞、配置不合规等安全风险。

  - 支持深入扫描

通过配置验证信息，可连接到服务器进行 OS 检测，进行多维度的漏洞、配置检测。

- 支持内网扫描

  可以通过跳板机方式访问业务所在的服务器，适配不同企业网络管理场景。

- 弱密码扫描应用场景

  主机或中间件等资产一般使用密码进行远程登录，攻击者通常使用扫描技术来探测其用户名和弱口令。

  - 多场景可用

    支持操作系统(RDP 协议、SSH 协议)、数据库（如 Mysql、Redis）等常见中间件服务的弱口令检测。

  - 丰富的弱密码库

    丰富的弱密码匹配库，模拟黑客对各场景进行弱口令探测。

- 中间件扫描应用场景

  中间件可帮助用户灵活、高效地开发和集成复杂的应用软件，一旦被黑客发现漏洞并利用，将影响上下层安全。

  - 丰富的扫描场景

    支持主流 Web 容器、前台开发框架、后台微服务技术栈的版本漏洞和配置合规扫描。

  - 多扫描方式可选

    支持通过标准包或者自定义安装等多种方式识别服务器的中间件及其版本，全方位发现服务器的漏洞风险。

- 内容合规检测应用场景

  当网站被发现有不合规言论时，会给企业造成品牌和经济上的多重损失。

  - 精确识别

    同步更新时政热点和舆情事件的样本数据，准确定位各种涉黄、涉暴涉恐、涉政等敏感内容。

  - 智能高效

    对文本、图片内容进行上下文语义分析，智能识别复杂变种文本。

1.6 使用约束

VSS 是通过公网访问域名/IP 地址进行扫描的，请确保该目标域名/IP 地址能通过公网正常访问。

扫描 IP 加入网站扫描白名单

如果您的网站设置了防火墙或其他安全策略，将导致 VSS 的扫描 IP 被当成恶意攻击者而误拦截。因此，在使用 VSS 前，请您将以下 VSS 的扫描 IP 添加至网站访问的白名单中：

114.217.39.79，222.93.127.109

1.7 计费说明

本小节主要介绍漏洞扫描服务的计费说明，包括计费项、计费模式、续费等。

计费项

VSS 根据您的 VSS 服务版本，扫描配额包的个数和购买时长计费。

表1-4 计费项信息

计费项目	计费说明
服务版本（必选）	按购买的服务版本（基础版、专业版、高级版或企业版）计费。
扫描配额包	按购买的个数计费。
购买时长	提供包年/包月和按需计费的购买模式。

计费模式

VSS 提供按需计费和包年/包月两种计费模式，用户可以根据实际需求选择计费模式。

表1-5 VSS 各服务版本计费方式

服务版本	支持的计费方式	说明
基础版	• 配额内的服务免费 • 按需计费	• 基础版配额内仅支持 Web 网站漏洞扫描（域名个数：5 个，扫描次数：每日 5 次）是免费的。 • 基础版提供的以下功能按需计费： 1. 可以将 Web 漏洞扫描或主机漏洞扫描任务升级为专业版规格进行扫描，扫描完成后进行一次性扣费。 2. 主机扫描一次最多支持 20 台主机。
专业版	包年/包月	相对于按需付费，包年/包月购买方式能够提供更大的折扣，对于长期使用者，推荐该方式。包周期计费为按照订单的购买周期来进行结算。不限制扫描次数。
高级版		
企业版		

变更配置

- 域名配额扩容：当您的业务需求增加，可在计费周期内“扩容”域名的扫描配额包。支持扩容**专业版配额**、**高级版配额**以及**企业版配额**。不支持多个版本同时存在。

- 专业版升级为高级版：当您是专业版用户时，如果需要将专业版扫描配额包中的二级域名配额全部升级为一级域名配额，可以直接将**专业版**升级为**高级版**。
- 退订：购买漏洞扫描服务的扫描配额包后，如需停止使用，

续费

扫描配额包到期后，您可以进行续费以延长扫描配额包的有效期，也可以设置到期自动续费。

到期与欠费

包周期资源开通成功后，如果没有按时续费，平台会提供一定的保留期。

欠费后，可以查看欠费详情。为防止相关资源不被停止或者释放，请及时进行充值，帐号将进入欠费状态，需要在约定时间内支付欠款。

1.8 个人数据保护机制

为了确保网站访问者的个人数据（例如用户名、密码等）不被未经过认证、授权的实体或者个人获取，VSS 通过加密存储个人数据、控制个人数据访问权限以及记录操作日志等方法防止个人数据泄露，保证您的个人数据安全。

收集范围

VSS 收集及产生的个人数据如表 1-6 所示。

表1-6 个人数据范围列表

类型	收集方式	是否可以修改	是否必须
域名/IP 地址	在添加域名时，由用户在界面输入。	是	是
用户名（网站登录）	在设置账号密码登录方式时，由用户在界面输入。	是	否
密码（网站登录）	在设置账号密码登录方式时，由用户在界面输入。	是	否
cookie 值	在设置 cookie 登录方式时，由用户在界面输入。	是	否 cookie 值可能不含有用户的个人信息。

存储方式

除域名/IP 地址明文保存外，其他字段加密存储。

访问权限控制

用户只能查看自己业务的相关信息。

1.9 VSS 权限管理

系统默认提供两种权限：用户管理权限和资源管理权限。

- 用户管理权限可以管理用户、用户组及用户组的权限。
- 资源管理权限可以控制用户对云服务资源执行的操作。

如果您需要对您所拥有的 VSS 进行精细的权限管理，您可以使用统一身份认证服务（Identity and Access Management，简称 IAM），通过 IAM，您可以：

- 根据企业的业务组织，在您的云帐号中，给企业中不同职能部门的员工创建 IAM 用户，让员工拥有唯一安全凭证，并使用 VSS 资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。

如果云帐号已经能满足您的要求，则不需要创建独立的 IAM 用户，不影响您使用 VSS 服务的其它功能。

1.10 术语解释

表1-7 术语表

术语	说明
漏洞（Vulnerability）	硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，可以使攻击者能够在未授权的情况下访问或破坏系统。
网站（Website）	网站（Website）开始是指在因特网上根据一定的规则，使用 HTML（标准通用标记语言下的一个应用）等工具制作的用于展示特定内容相关网页的集合。简单地说，网站是一种沟通工具，人们可以通过网站来发布自己想要公开的资讯，或者利用网站来提供相关的网络服务。
Web 应用（Web App）	Web 应用程序是可使用任何 Web 浏览器访问的软件或程序。Web 应用程序是具有功能和交互式元素的网站。
主机（Host）	连接了硬盘、硬盘子系统或者文件服务器，并能在其上存储数据和 I/O 访问的计算机系统。大型机、服务

术语	说明
	器、工作站以及个人电脑，甚至多处理器机器和集群计算机系统都被称为主机。
安全配置基线（Security Configuration Baseline）	安全配置基线即针对不同的产品或者系统，依据安全评估标准，形成一系列固化的检查规则、评估方法，为安全管理人员在实际的安全配置工作中提供参考和标杆。
NVD	National Vulnerability Database，国家安全漏洞库。
CVE（Common Vulnerabilities and Exposures）	又称通用漏洞披露、常见漏洞与披露，是一个与信息安全有关的数据库，收集各种信息安全弱点及漏洞并给予编号以便于公众查阅。
安全通告（Security Advisory）	安全通告包含漏洞严重等级、业务影响和修补方案等信息，用以传递漏洞修补方案。一般用于厂商披露器产品直接相关的漏洞。
IAM	Identity and Access Management，统一身份认证服务。

2 操作指引

漏洞扫描服务使用概览如表 2-1 所示。

表2-1 漏洞扫描服务使用流程概览

子流程	说明
购买漏洞扫描服务	漏洞扫描服务提供了基础版、专业版、高级版和企业版四种服务版本。其中，基础版配额内的服务免费，部分功能按需计费；专业版、高级版和企业版需要收费。 具体操作请参见购买漏洞扫描服务。
域名认证	具体操作请参见域名认证。
创建扫描任务	创建扫描任务即可对网站进行扫描，具体操作请参见创建扫描任务。
开启主机扫描	开启主机扫描即可对主机进行扫描，具体操作请参见开启主机扫描。
新增监测任务	新增监测任务即可对资产进行监测，具体操作请参见新增监测任务。
查看扫描结果	扫描完成后可以通过“任务详情”页面查看扫描结果。 • 网站扫描结果，请参见查看网站扫描详情。 • 主机扫描结果，请参见查看主机扫描详情。

3 开通 VSS

3.1 产品规格差异

漏洞扫描服务提供了基础版、专业版、高级版和企业版四种服务版本。其中，基础版配额内的服务免费，部分功能按需计费；专业版、高级版和企业版需要收费。

VSS 各服务版本支持的计费方式、功能和规格说明如下所示，您可以根据业务需求选择相应的服务版本。

表3-1 VSS 各服务版本计费方式

服务版本	支持的计费方式	说明
基础版	• 配额内的服务免费 • 按需计费	• 基础版配额内仅支持 Web 网站漏洞扫描（域名个数：5 个，扫描次数：5 个域名每日总共可以扫描 5 次）是免费的。 • 基础版提供的以下功能按需计费： 1. 可以将 Web 漏洞扫描或主机漏洞扫描任务升级为专业版规格进行扫描，扫描完成后进行一次性扣费。 2. 主机扫描一次最多支持 20 台主机。
专业版	包年/包月	相对于按需付费，包年/包月购买方式能够提供更大的折扣，对于长期使用者，推荐该方式。包周期计费为按照订单的购买周期来进行结算。
高级版		
企业版		

表3-2 VSS 各服务版本功能说明

功能	基础版	专业版	高级版	企业版
常见 Web 漏洞检测	√	√	√	√
端口扫描	√	√	√	√

功能	基础版	专业版	高级版	企业版
CVE 漏洞扫描	√	√	√	√
自定义登录方式	√	√	√	√
Web 2.0 高级爬虫	√	√	√	√
网站指纹识别	√	√	√	√
扫描任务管理	√	√	√	√
漏洞查看及管理	√	√	√	√
弱密码检测	×	√	√	√
网页内容合规检测（文字）	×	√	√	√
操作系统漏洞扫描	×	√	√	√
操作系统基线检查	×	√	√	√
中间件基线检查	×	√	√	√
查看漏洞修复建议	×	√	√	√
下载扫描报告	×	√	√	√
安全监测（定时扫描）	×	√	√	√
网页内容合规检测（图片）	×	×	×	√
网站挂马检测	×	×	×	√
链接健康检测（死链、暗链、恶意外链）	×	×	×	√
操作系统等保合规检查	×	×	×	√
支持手动探索文件导入	×	×	×	√

表3-3 VSS 各服务版本支持的扫描配额说明

版本	域名/IP 个数	单个任务时长	任务优先级	单用户并发扫描数
基础版	Web 漏扫：包含 5 个二级域名或 IP:端口。 Web 漏扫：5 个域名每日总共可以扫描 5 次。	2 小时	低	默认 Web 漏扫最大并发为 1 个域名。
专业版	Web 漏扫：包含 1 个二级域名或 IP:端口。	无限制	高	默认 Web 漏扫最大并发为 3 个

版本	域名/IP 个数	单个任务时长	任务优先级	单用户并发扫描数
	主机漏扫：包含 20 个 IP 地址。			域名。 默认主机漏扫最大并发为 5 个 IP。
高级版	Web 漏扫：默认包含 1 个一级域名（不限制下属二级域名个数）/IP（不限制端口个数）。 主机漏扫：不限制 IP 地址个数。	无限制	高	默认 Web 漏扫最大并发为 5 个域名。 默认主机漏扫最大并发为 10 个 IP。
企业版	Web 漏扫：默认包含 5 个一级域名（不限制下属二级域名个数）/IP（不限制端口个数）。 主机漏扫：不限制 IP 地址个数。 说明 当默认的扫描配额不能满足您的需求时，您可以通过购买扫描配额包增加扫描配额（一个扫描配额包中包含一个一级域名扫描配额）。	无限制	高	默认 Web 漏扫最大并发为 10 个域名。 默认主机漏扫最大并发为 20 个 IP。 说明 更高并发需要，请提交工单联系专业工程师为您服务。

3.2 购买漏洞扫描服务

操作场景

该任务指导用户首次使用 VSS 时，如何购买漏洞扫描服务的专业版、高级版和企业版扫描功能。

须知

- 仅支持从专业版升级至高级版，当您是专业版用户时，如果需要将专业版扫描配额包中的二级域名配额升级为一级域名配额，可以直接将专业版升级到高级版。
- 不支持多个版本同时存在。
- 不支持从专业版或高级版直接升级至企业版，当您是专业版或高级版用户时，如果需要使用企业版，请直接购买企业版。为保证您的权益，请您购买企业版后，提工单退订专业版或高级版。
- 购买漏洞扫描服务或配额后，不支持直接修改配额，仅支持升级规格，请谨慎操作。

前提条件

已获取管理控制台的登录帐号与密码。

购买步骤

步骤 1 登录管理控制台。

步骤 2 在页面上方选择区域或项目后，单击 ☰，选择“安全 > 漏洞扫描服务”，进入漏洞扫描服务管理界面。

说明

- 首次使用 VSS，您可以在页面左侧，单击“立即购买”，进入 VSS 购买页面。
- 如果您已经体验了 VSS 基础版，请在页面的右上角，单击“升级规格”，进入 VSS 购买页面。

步骤 3 在购买漏洞扫描服务界面，进行服务选型配置。

- “计费模式”选择“包年/包月”，如图 3-1、图 3-2 和图 3-3 所示，参数说明如表 3-4 所示，参数配置完成后，请执行步骤 4。

说明

- 使用基础版的用户，可以继续使用基础版的功能，每个用户可添加的域名个数不超过 5 个。
- 当用户在使用中需要增加专业版/高级版/企业版域名扫描配额，购买的数量不能小于已购买的数量，到期时间不变。

图3-1 计费模式-包年/包月（专业版）

图3-2 计费模式-包年/包月（高级版）

图3-3 计费模式-包年/包月（企业版）

表3-4 服务选型参数说明

参数	参数说明
规格选择	漏洞扫描服务提供了基础版、专业版、高级版和企业版四种服务版本。其中，基础版配额内的服务免费，部分功能按需计费；专业版、高级版和企业版需要收费。
规格说明	对应版本支持的功能介绍。
购买时长	• 专业版 可以选择 1 个月～3 年的时长。 • 高级版 可以选择 1 个月～3 年的时长。 • 企业版 支持“1 个月”、“3 个月”、“1 年”的购买时长。
扫描配额包	• 选择“专业版”时，需要配置购买的域名扫描配额包数量。 Web 漏扫：包含 1 个二级域名或 IP:端口，每个公网 IP 支持的端口号不限 主机漏扫：包含 20 个 IP 地址。 购买的“扫描配额包”不能少于资产列表的网站数量。 须知 • 如果您在购买专业版之前使用过免费体验版（即基础版）进行扫描，在购买专业版时，“扫描配额包”的选择必须等于或者大于当前资产列表已添加的网站个数。 • 如果当前资产列表的某个基础版域名，您不想升级为专业版为其付费，请您在购买专业版之前对其进行删除。 • 如果您只需要将当前基础版域名全部升级为专业版规格，“扫描配额包”

参数	参数说明
	的选择等于当前资产列表已添加的网站个数。 • 如果您需要增加域名配额，即增加扫描的网站个数，“扫描配额包”的选择大于当前资产列表已添加的网站个数，且“扫描配额包”的选择值为您期望的域名配额值。 • 购买专业版成功后，当前资产列表所有基础版域名默认升级为专业版，享受专业版规格。 • 选择“高级版”时，需要配置购买的域名扫描配额包数量。 Web 漏扫：默认包含 1 个一级域名（不限制二级域名个数）/IP（不限制端口个数），每个公网 IP 支持的端口号不限。 主机漏扫：不限制 IP 地址个数。 • 选择“企业版”时，每个配额包包含如下： Web 漏扫：默认包含 5 个一级域名（不限制二级域名个数）/IP（不限制端口个数），每个公网 IP 支持的端口号不限。 主机漏扫：不限制 IP 地址个数 若默认的域名配额数量不能满足您的要求，您可以通过配置扫描配额包的数量，增加域名配额。

- 计费模式选择“按需计费”，如图 3-4 所示。
  - 创建任务时，保持升级开关关闭，开始扫描后默认享受单次基础版扫描服务。
  - 创建任务时，开启升级开关，开始扫描后享受单次专业版扫描服务。扫描开始后进行一次性扣费，请保障您的账户余额充足。
  - 基于基础版创建主机扫描时，每次扫描最多 20 台主机，扫描开始后进行一次性扣费，请保障您的账户余额充足。

图3-4 计费模式-按需计费

请参照以下操作步骤完成一次扫描任务：

a. 单击“立即体验”回到“资产列表”界面。

说明

如果没有域名，请先添加域名并完成域名认证，再在创建任务界面进行单次按需购买。

b. 单击“扫描”，进入“创建任务”界面，相关设置如图 3-5 所示。

图3-5 扫描设置

您可以打开“是否将本次扫描升级为专业版规格”开关，将本次扫描升级为专业版。

设置完成后，用户可以根据需要选择定时扫描或者立即扫描，在弹出的“付费提醒”界面，单击“同意并扫描”。

步骤 4 参数设置完毕后，在页面右下角，单击“立即购买”。

步骤 5 确认订单详情无误后，单击“去支付”。

如果订单填写有误，用户可以单击“上一页”，回到服务选型页面修改配置信息后再继续购买。

步骤 6 在“付款”页面，选择付款方式进行付款。

----结束

3.3 域名配额扩容

操作场景

该任务指导已购买专业版、高级版或者企业版的用户增加扫描的域名配额。

须知

- 若用户以前使用过基础版（免费体验版）进行扫描，在升级为专业版时，基础版所有的已有域名会占用专业版配额。
- 当前不支持从专业版或者高级版直接升级至企业版，若您是专业版或者高级版用户，并想要使用企业版，请直接购买企业版，为保证您的权益，请您购买企业版后，提工单退订专业版或者高级版。
- 当前不支持仅购买企业版（不购买配额）后再次升级增加配额。如果要想增加配额，请先退订企业版，重新购买。

前提条件

- 已获取管理控制台的登录帐号和密码。
- 已购买专业版、高级版或者企业版的漏洞扫描服务。

扩容专业版配额

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击 ☰，选择“安全 > 漏洞扫描服务”，进入漏洞扫描服务页面。

步骤 3 在左侧导航栏，选择“资产列表”，单击右上角的“升级规格”，进入升级专业版规格入口。

步骤 4 在升级规格界面设置配额。

在“扫描配额包”栏，单击 + 增加域名扫描配额包数量。

说明

- “扫描配额包”即配置的域名/IP 地址个数，目前支持的范围为 1-100。
- 选择的“扫描配额包”必须大于当前拥有的域名配额。
- 每个扫描配额包默认包含 1 个二级域名或公网 IP:端口。

步骤 5 在页面右下角，单击“立即购买”。

步骤 6 确认订单详情无误后，单击“去支付”。

如果订单填写有误，用户可以单击“上一页”，回到服务选型页面修改配置信息后再继续购买。

步骤 7 在“付款”页面，选择付款方式进行付款。

----结束

扩容高级版配额

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击 ，选择“安全 > 漏洞扫描服务”，进入漏洞扫描服务页面。

步骤 3 在左侧导航栏，选择“资产列表”，单击右上角的“升级规格”，进入升级高级版规格入口。

步骤 4 在升级规格界面设置配额。

在“扫描配额包”栏，单击 增加域名扫描配额包数量。

说明

- “扫描配额包”即配置的域名/IP 地址个数，目前支持的范围为 1-100。
- 选择的“扫描配额包”必须大于当前拥有的域名配额。
- 每个扫描配额包默认包含 1 个一级域名（不限制二级域名个数）/IP（不限制端口个数）。

步骤 5 在页面右下角，单击“立即购买”。

步骤 6 确认订单详情无误后，单击“去支付”。

如果订单填写有误，用户可以单击“上一页”，回到服务选型页面修改配置信息后再继续购买。

步骤 7 在“付款”页面，选择付款方式进行付款。

----结束

扩容企业版配额

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击 ，选择“安全 > 漏洞扫描服务”，进入漏洞扫描服务页面。

步骤 3 在左侧导航栏，选择“资产列表”，单击右上角的“升级规格”，进入升级企业版规格入口。

步骤 4 在升级规格界面设置配额。

在“扫描配额包”栏，单击 增加扫描配额包 。

说明

- “扫描配额包”即配置的域名/IP 地址个数，目前支持的范围为 1～100。
- 每个扫描配额包默认包含 1 个一级域名（不限制二级域名个数）/IP（不限制端口个数）。

步骤 5 在页面右下角，单击“立即购买”。

步骤 6 确认订单详情无误后，单击“去支付”。

如果订单填写有误，用户可以单击“上一页”，回到服务选型页面修改配置信息后再继续购买。

步骤 7 在“付款”页面，选择付款方式进行付款。

----结束

3.4 升级为高级版

当您是专业版用户时，如果需要将专业版扫描配额包中的二级域名配额全部升级为一级域名配额，可以直接将专业版升级为高级版。

该任务指导专业版用户将漏洞扫描服务升级为高级版。

前提条件

- 已获取管理控制台的登录帐号和密码。
- 已购买专业版的漏洞扫描服务。

升级为高级版

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击 ☰，选择“安全 > 漏洞扫描服务”，进入漏洞扫描服务页面。

步骤 3 单击“升级规格”，进入升级规格界面。

步骤 4 在升级规格界面，单击“高级版”，设置配额。

在“扫描配额包”栏，单击 + 增加域名扫描配额包数量。

说明

- “扫描配额包”即配置的域名/IP 地址个数，目前支持的范围为 1-100。
- “扫描配额包”栏的数量默认为专业版配额的数量。
- “扫描配额包”可以选择大于或等于当前拥有的专业版配额，VSS 仅支持专业版配额全部升级，不支持专业版配额部分升级。
- 每个扫描配额包默认包含 1 个一级域名（不限制二级域名个数）/IP（不限制端口个数）。

步骤 5 确认订单详情无误后，单击“去支付”。

如果订单填写有误，用户可以单击“上一页”，回到服务选型页面修改配置信息后再继续购买。

步骤 6 在“付款”页面，选择付款方式进行付款。

----结束

4 快速入门

4.1 如何使用漏洞扫描服务？

- 漏洞扫描服务（Vulnerability Scan Service，简称 VSS）是针对网站和主机进行漏洞扫描的一种安全检测服务，目前提供通用漏洞检测和漏洞生命周期管理服务。
- 用户新建任务后，即可人工触发扫描任务，检测出网站的漏洞并给出漏洞修复建议。
- 本指南指导您快速上手漏洞扫描服务。

购买漏洞扫描服务

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击 ☰，选择“安全 > 漏洞扫描服务”，进入漏洞扫描服务页面。

步骤 3 单击“升级规格”，进入购买页面，选择计费模式、服务版本、购买时长和扫描包数量。

后面操作以“企业版”为例进行介绍。

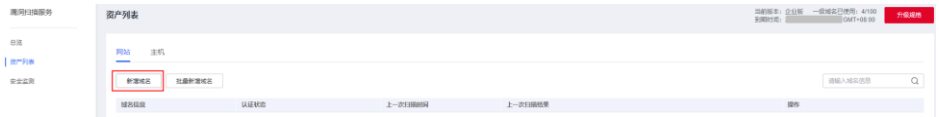
说明

漏洞扫描服务提供基础版、专业版、高级版和企业版扫描服务，基础版可免费使用，但是功能和规格受限，专业版、高级版和企业版需付费。

----结束

新增域名

步骤 1 在左侧导航树中，选择“资产列表”，在域名列表的左上角，单击“新增域名”。



步骤 2 域名信息配置，填写域名名称和“域名/IP 地址”。

步骤 3 单击“确认”，进入域名认证页面。

步骤 4 选择“免认证”，单击“完成认证”。

步骤 5 （可选）根据实际情况完成网站设置。

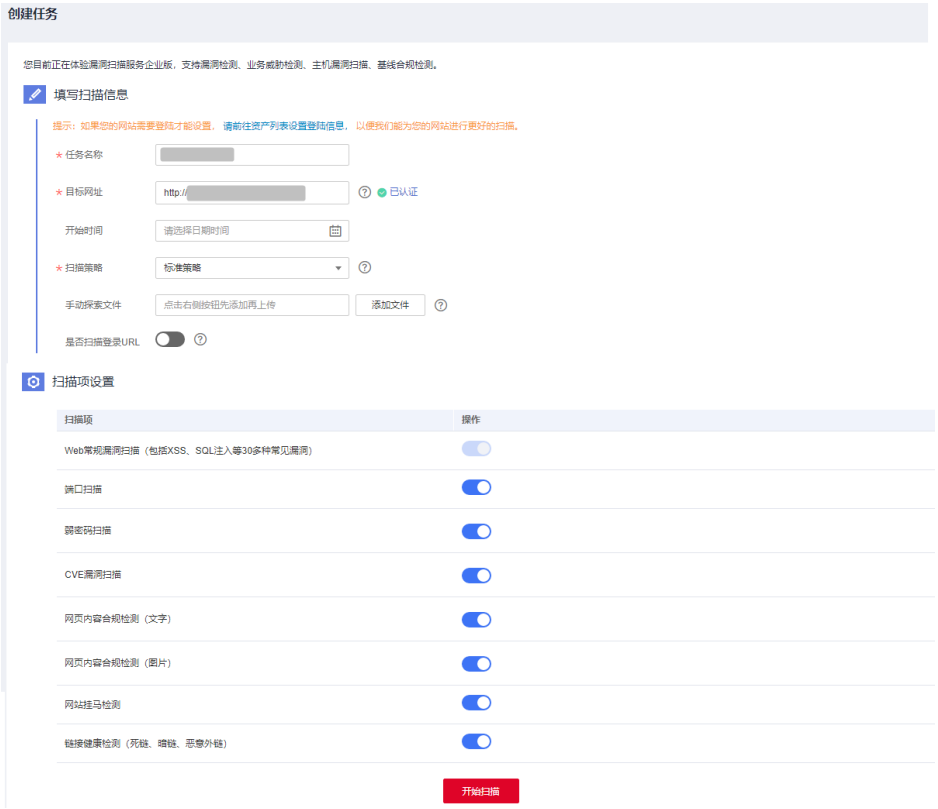
如果网站中某些网页需要登录才能访问，请您进行登录设置，以便 VSS 能够为您发现更多安全问题。

----结束

创建扫描任务

步骤 1 域名认证成功后，在目标域名的“操作”列，单击“扫描”。

步骤 2 填写域名信息，设置开始扫描时间，选择扫描模式。



步骤 3　设置完成后，单击“开始扫描”。

说明

如果您目前为基础版，只是需要享受单次专业版扫描服务，请打开“是否将本次扫描升级为专业版规格”开关。

----结束

查看扫描结果

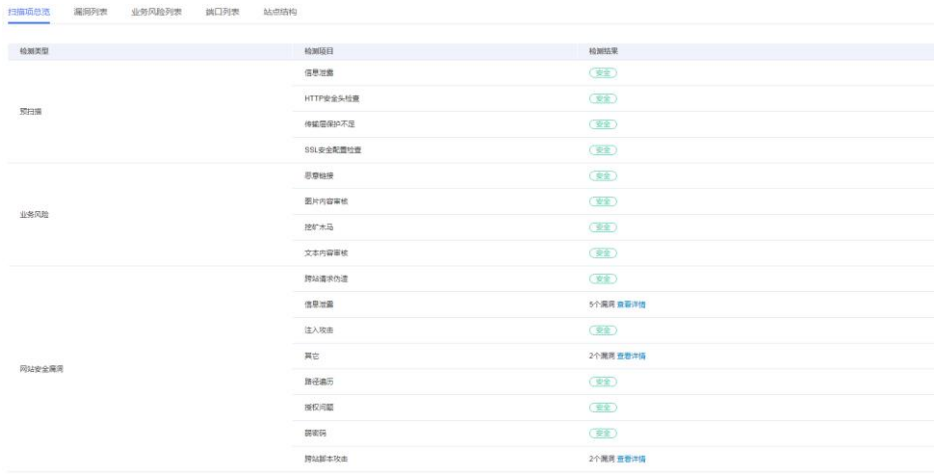
步骤 1　在目标域名所在行的“上一次扫描结果”列，单击分数，进入扫描结果界面。

步骤 2　单击“生成报告”，生成网站扫描报告。

如果报告已生成，则可跳过此步。扫描报告仅支持专业版及以上版本扫描任务下载，请升级到正式版及以上版本体验。

步骤 3 单击“下载报告”，查看详细的检测报告。

步骤 4 分别查看扫描项总览、漏洞列表、业务风险列表、端口列表、站点结构。



说明

基础版不支持下载报告功能，为了更好的防护您的资产，建议您购买专业版或者企业版漏洞扫描服务。

----结束

5 网站漏洞扫描

5.1 添加域名

开通漏洞扫描服务后，您首先需要将网站资产以 IP 或域名的形式添加到漏洞扫描服务中并完成域名认证，才能进行漏洞扫描。

如果您的网站中存在需要登录才能访问的网页，还需要配置网站登录信息（“账号密码登录”和“cookie 登录”两种登录方式），VSS 才能为您更好的检测网站安全问题。

说明

如果您在添加域名时，提示“当前套餐可新增域名已达到上限”，无法添加域名时，可参照以下方法进行处理：

- 参照域名配额扩容进行域名配额扩容，购买“扫描配额包”，“扫描配额包”必须大于当前版本已有的配额。
- 如果您的资产列表有不需要防护的域名，建议删除后再添加新的域名。

前提条件

已获取管理控制台的登录帐号与密码。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击 ☰，选择“安全 > 漏洞扫描服务”，进入漏洞扫描服务页面。

步骤 3 在“资产列表 > 网站”页签，单击“新增域名”，进入添加域名入口。

步骤 4 在弹出的对话框中，添加“域名/IP 地址”，设置“域名别称”，如图 5-1 所示。

域名别称：帮助用户识别自己的域名地址，您可以填写任意方便您识别网站域名的名称。

图5-1 新增域名

步骤 5　单击“确认”，进行域名所有权认证。

说明

- 如果暂时不进行域名所有权认证，可关闭对话框，后续参照域名认证章节完成域名认证。
- 如果待检测站点的服务器搭建在云上，且该服务器是您当前登录帐号的资产，才可以选择“一键认证”的方式进行快速认证，否则只能选择“免认证”的方式进行认证。

- 免认证，仔细阅读图 5-2 中的使用须知，确认符合条件后，完成域名认证。

图5-2 免认证方式

- 一键认证，如图 5-3 所示。

图5-3 一键认证方式

单击“完成认证”，进行域名认证，执行完成后，该域名的状态为“已认证”。

步骤 6 如果域名认证成功，页面跳转到“网站设置”页面，参照表 5-1 完成网站信息配置，如图 5-4 所示。

说明

- 如果网站中存在需要登录才能访问的网页，进行登录设置后，VSS 能够为您更好的检测网站安全问题，后续也可以参照编辑域名进行配置。
- VSS 提供了“账号密码登录”和“cookie 登录”两种登录方式，为了提高登录成功率，建议您配置两种登录方式。

图5-4 网站登录设置

表5-1 网站登录页面参数说明

参数名称	参数说明	样例
“登录方式一：账号密码登录”		
登录页面	网站登录页面的地址。	https://auth.example.com/
用户名	登录网站的用户名。	vsstest
密码	对应用户名的密码。	--
确认密码	再次输入用户名的密码。	--
“登录方式二：cookie 登录” 如果网站登录需要动态验证码才能登录成功，此时必须配置“cookie 登录”方式。		
cookie 值	输入登录网站的 cookie 值。	domain_tag
“网站登录验证”		
验证登录网址	登录成功后才能访问的网址，便于 VSS 快速判断您的登录信息是否有效。	https://console.example.com/
高级配置		
自定义 Header	配置 HTTP 请求头部。最多可添加 5 个自定义 HTTP 请求头。 当待扫描的网站需要请求中附带特殊的 HTTP 请求头时，可以通过自定义 Header 进行设置。	--

步骤 7 单击“确认”。

----结束

后续操作

网站登录方式设置完成，您还需要创建扫描任务，详细操作请参见创建扫描任务。

5.2 域名认证

该任务指导用户通过漏洞扫描服务完成域名认证。

前提条件

- 已获取管理控制台的登录帐号与密码。
- 域名的“认证状态”为“未认证”。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击 ☰，选择“安全 > 漏洞扫描服务”，进入漏洞扫描服务页面。

步骤 3 在“资产列表 > 网站”页签，单击对应的网站信息“去认证”。

步骤 4 进入域名认证入口，如图 5-5 所示。

图5-5 进入域名认证页面

步骤 5 在弹出的“认证域名”对话框中，选择域名认证方式完成域名认证。

- 一键认证，如图 5-6 所示。

图5-6 一键认证方式

步骤 6 单击“完成认证”，进行域名认证。

执行完成后，该域名的状态为“已认证”。

----结束

5.3 网站登录设置

操作场景

该任务指导用户通过漏洞扫描服务进行网站登录设置，修改网站信息。

如果您的网站页面需要登录才能访问，必须进行网站登录设置，以便 VSS 能为您发现更多安全问题。VSS 提供了两种登录方式，请您根据您的网站访问限制条件选择登录方式：

- 方式一：账号密码登录。

  如果您的网站仅需要账号密码就可以登录访问，设置方式一即可。
- 方式二：cookie 登录。

  如果您的网站除了需要账号密码登录，还有其他的访问限制，如需要输入“动态验证码”，必须选择方式二，设置 cookie 登录。

须知

- 若没有 cookie，请在“高级配置”中，通过添加自定义 Header 的方式进行登录扫描。
- 若没有 cookie，也没有自定义 Header，则 VSS 不支持扫描该网站。

以上登录方式根据网站访问情况可二选一。

前提条件

- 已获取管理控制台的登录帐号与密码。
- 已添加域名。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击 ☰，选择“安全 > 漏洞扫描服务”，进入漏洞扫描服务页面。

步骤 3 在“资产列表 > 网站”页签，单击对应的网站信息“操作”列的“编辑”。

步骤 4 进入网站登录设置入口，如图 5-7 所示。

图5-7 进入网站登录设置入口

步骤 5 在域名编辑页面，根据需要修改“网站信息”和“网站登录设置”，如图 5-8 所示，参数说明如表 5-2 所示。

图5-8 编辑网站登录信息页面

表5-2 参数说明

参数名称	参数说明
网站信息修改	
域名/IP 地址	未认证的域名可修改。 说明 VSS 不支持修改已认证域名的“域名/IP 地址”，如需修改，请删除域名后，重新创建新的域名。

参数名称	参数说明
域名别称	自定义的域名名称，可修改。
网站登录设置 如果您的网站页面需要登录才能访问，请您进行登录设置，以便 VSS 能为您发现更多安全问题。 • 如果您的网站仅需要账号密码就可以登录访问，设置方式一即可。 • 如果您的网站除了需要账号密码登录，还有其他的访问限制，如需要输入动态验证码，必须设置方式二。	
“登录方式一：账号密码登录”	
登录页面	网站登录页面的地址。
用户名	登录网站的用户名。
密码	用户名的密码。
确认密码	再次输入用户名的密码。
“登录方式二：cookie 登录”	
cookie 值	输入登录网站的 cookie 值。 说明 • 若使用 cookie 登录时，没有获取到 cookie 值，您可以在“高级配置”中通过添加自定义 Header 的方式进行登录。 • 添加自定义 Header 时，请获取会话相关的 HTTP 请求头。常见的如：带有 Token 或 Session 字样的 HTTP 请求头。
验证登录网址	登录成功后才能访问的网址，便于 VSS 快速判断您的登录信息是否有效。
“高级配置”	
自定义 Header	配置 HTTP 请求头部。最多可添加 5 个自定义 HTTP 请求头。 当待扫描的网站需要请求中附带特殊的 HTTP 请求头时，可以通过自定义 Header 进行设置。

步骤 6 单击“确认”。

----结束

5.4 创建扫描任务

操作场景

该任务指导用户通过漏洞扫描服务创建扫描任务。

前提条件

- 已获取管理控制台的登录帐号与密码。
- 域名的“认证状态”为“已认证”。
- 如果您的网站设置了防火墙或其他安全策略，将导致 VSS 的扫描 IP 被当成恶意攻击者而误拦截。因此，在使用 VSS 前，请您将以下 VSS 的扫描 IP 添加至网站访问的白名单中：

  114.217.39.79，222.93.127.109

操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击 ☰，选择“安全 > 漏洞扫描服务”，进入漏洞扫描服务页面。

步骤 3 在“资产列表 > 网站”页签，单击对应的网站信息“操作”列的“扫描”。

步骤 4 进入创建扫描任务入口，如图 5-9 所示。

图5-9 进入创建扫描任务入口

步骤 5 在“创建任务”界面，请根据表 5-3 进行扫描设置，设置后如图 5-10 所示。

图5-10 创建扫描任务

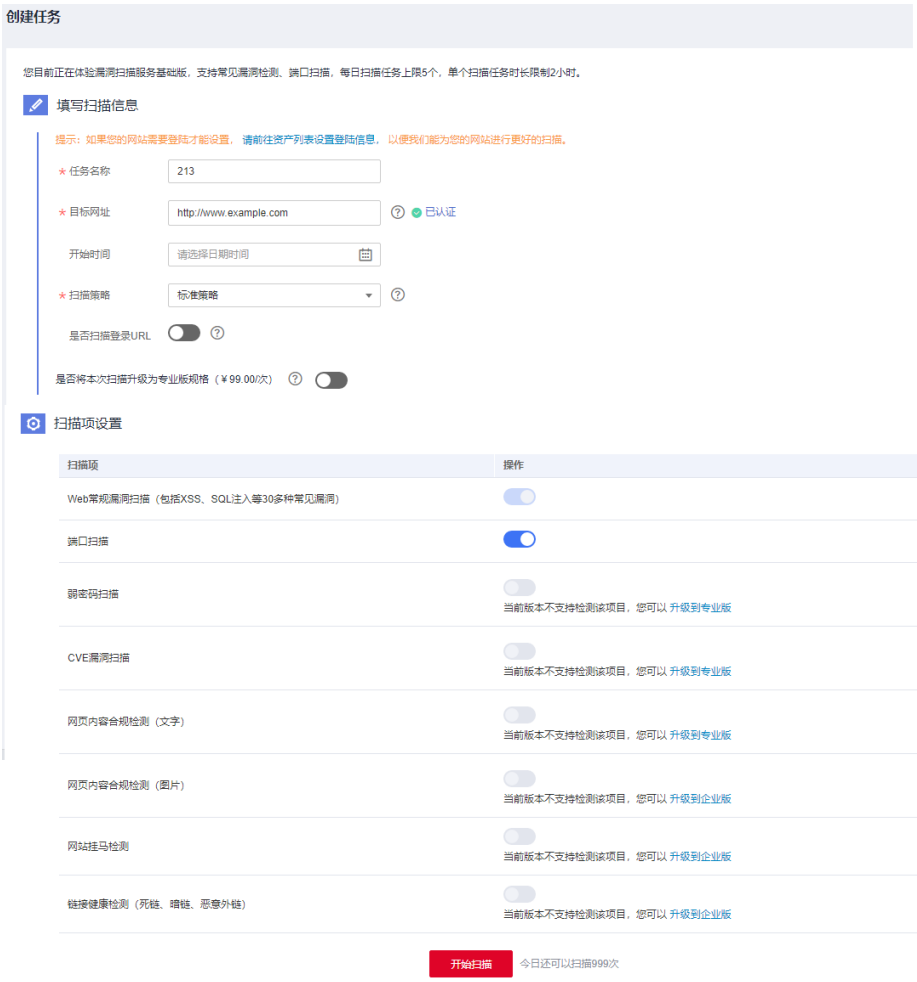


表5-3 扫描设置参数说明

参数	参数说明
任务名称	用户自定义。
目标网址	待扫描的网站地址或 IP 地址。 通过下拉框选择已认证通过的域名。
开始时间	可选参数，设置开始扫描的时间，不设置默认立即扫描。
扫描策略	三种扫描策略： • 极速策略：扫描耗时最少，能检测到的漏洞相对较少。 • 标准策略：扫描耗时适中，能检测到的漏洞相对较多。 • 深度策略：扫描耗时最长，能检测到最深处的漏洞。 有些接口只能在登录后才能访问，建议用户配置对应接口的用户名和密码，VSS 才能进行深度扫描。 **说明**

参数	参数说明
	• “极速策略”：扫描的网站 URL 数量有限且 VSS 会开启耗时较短的扫描插件进行扫描。 • “深度策略”：扫描的网站 URL 数量不限且 VSS 会开启所有的扫描插件进行耗时较长的遍历扫描。 • “标准策略”：扫描的网站 URL 数量和耗时都介于“极速策略”和“深度策略”两者之间。
是否扫描登录 URL	默认不扫描登录 URL，开启扫描登录 URL 前请先评估业务影响。
是否将本次扫描升级为专业版规格	基础版用户开启此功能后，扫描过程中会按需扣费： • 鼠标移动至 了解升级后影响。 • 打开此功能时，扫描时会自动升级为专业版按需扣费，关闭该功能时，扫描时不会升级。
扫描项设置	VSS 支持的扫描功能参照表 5-4。 • ：开启。 • ：关闭。

表5-4 扫描项设置

扫描项名称	说明
Web 常规漏洞扫描（包括 XSS、SQL 注入等 30 多种常见漏洞）	提供了常规的 30 多种常见漏洞的扫描，如 XSS、SQL 等漏洞的扫描。默认为开启状态，不支持关闭。
端口扫描	检测主机打开的所有端口。
弱密码扫描	对网站的弱密码进行扫描检测。
CVE 漏洞扫描	CVE，即公共暴露漏洞库。VSS 可以快速更新漏洞规则，扫描最新漏洞。
网页内容合规检测（文字）	对网站文字的合规性进行检测。
网页内容合规检测（图片）	对网站图片的合规性进行检测。
网站挂马检测	挂马：上传木马到网站上，使得网站在运行的时候执行木马程序，被黑客控制，遭受损失。VSS 可以检测网站是否存在挂马。
链接健康检测（死链、	对网站的链接地址进行健康性检测，避免您的网站出现死

扫描项名称	说明
暗链、恶意外链）	链、暗链、恶意链接。

说明

- 如果您当前的服务版本已经为专业版，不会提示升级。
- 基础版支持常见漏洞检测、端口扫描，每日扫描任务上限 5 个，单个扫描任务时长限制 2 小时。
- 专业版支持常见漏洞检测、端口扫描、弱密码扫描，每日扫描任务上限多达 60 次。
- 高级版支持常见漏洞检测、端口扫描、弱密码扫描，每日扫描任务上限多达 60 次。
- 企业版支持常见网站漏洞扫描、基线合规检测、弱密码、端口检测、紧急漏洞扫描、周期性检测，每日扫描任务上限多达 60 次。

步骤 6 设置完成后，单击“开始扫描”。

说明

如果没有设置开始扫描时间，且此时服务器没有被占用，则创建的任务可立即开始扫描，任务状态为“进行中”；否则进入等待队列中等待，任务状态为“等待中”。

----结束

后续处理

扫描任务完成，您可以查看网站详情并下载网站扫描报告，详细操作请参见查看网站扫描详情、下载网站扫描报告。

5.5 查看网站扫描详情

该任务指导用户通过漏洞扫描服务查看网站扫描结果，可以查看扫描项总览、业务风险列表、漏洞列表、端口列表、站点结构。

VSS 暂不支持 web_CMS 漏洞扫描功能。

前提条件

- 已获取管理控制台的登录帐号与密码。
- 已添加域名并已完成域名认证。
- 已执行扫描任务。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击 ☰，选择“安全 > 漏洞扫描服务”，进入漏洞扫描服务页面。

步骤 3 在“资产列表 > 网站”页签，进入网站列表入口，如图 5-11 所示。

图5-11 进入网站列表入口

步骤 4 查看网站资产列表，相关参数说明如表 5-5 所示。

表5-5 网站资产列表参数说明

参数	参数说明
域名信息	• 域名/IP 地址 • 域名别称
认证状态	• “已认证” 目标域名已完成域名认证。 • “未认证” 目标域名未完成域名认证。单击“去认证”进行域名认证。
上次扫描时间	域名最近一次扫描任务的时间。
上一次扫描结果	域名最近一次扫描结果信息，包括得分和各等级的漏洞数量。单击得分或者“查看详情”，进入“扫描详情”界面查看扫描概况。

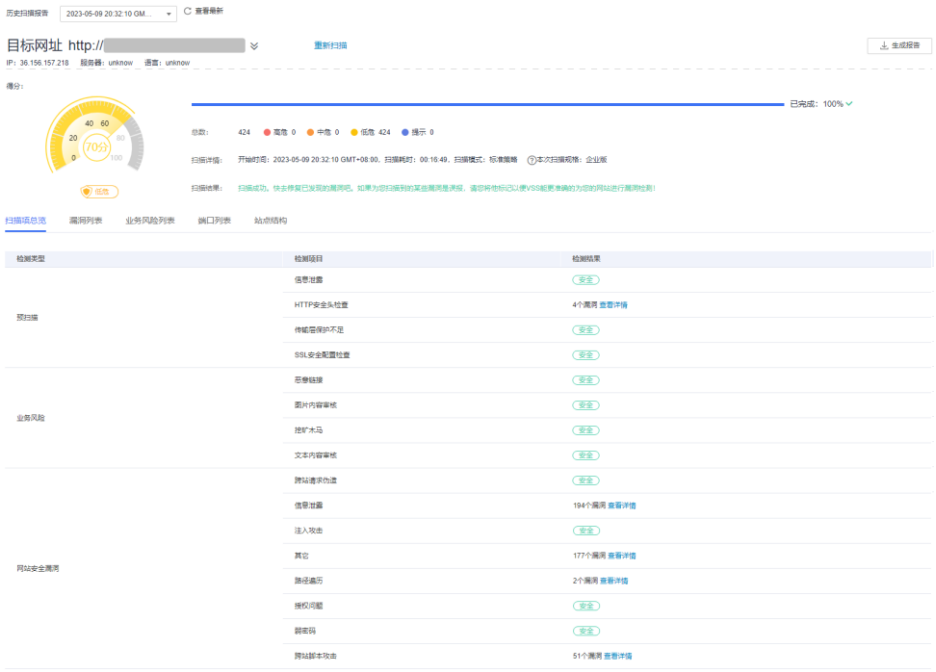
步骤 5 在目标域名所在行的“上一次扫描结果”列，单击分数或者“查看详情”，查看扫描任务详情，如图 5-12 所示。

说明

- 扫描任务详情界面默认显示最近一次的扫描情况，如果您需要查看其他时间的扫描情况，在“历史扫描报告”下拉框中，选择扫描时间点。
- 单击“重新扫描”，可以重新执行扫描任务。
- 当扫描任务成功完成后，单击右上角的“生成报告”，生成网站扫描报告后，单击右上角的 

，可以下载任务报告，目前只支持 PDF 格式。

图5-12 查看扫描任务详情



步骤 6 选择“扫描项总览”页签，查看扫描项的检测结果，如图 5-13 所示。

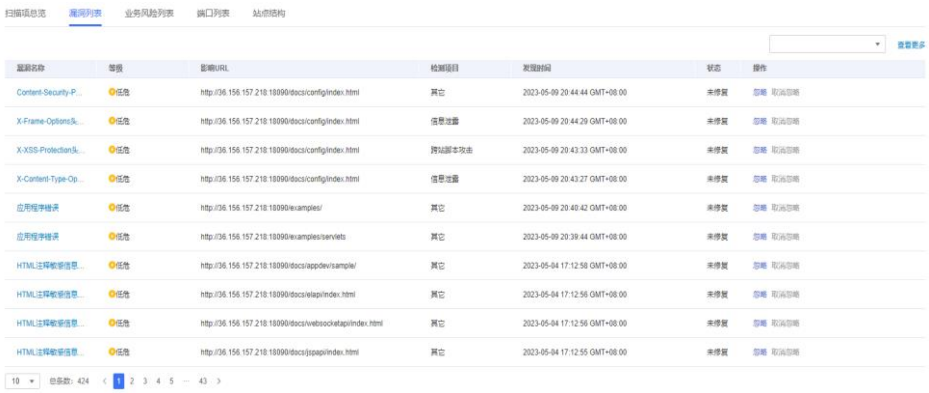
图5-13 扫描项总览

说明

如果检测结果存在漏洞或者风险，可在“检测结果”列，单击“查看详情”了解漏洞或者风险的详细情况。

步骤 7 选择“漏洞列表”页签，查看漏洞信息，如图 5-14 所示。

图5-14 漏洞列表



说明

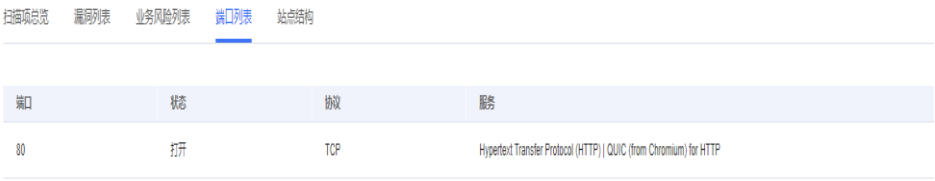
- 单击“查看更多”，可以查看详细的漏洞分析。
- 单击漏洞名称可以查看相应漏洞的“漏洞详情”、“漏洞简介”、“修复建议”。
- 如果您确认扫描出的漏洞不会对网站造成危害，请在目标漏洞所在行的“操作”列，单击“忽略”，忽略该漏洞，后续执行扫描任务会扫描出该漏洞，但扫描结果将不会统计忽略的漏洞。例如，如果您对 2 个低危漏洞执行了“忽略”操作，则再次执行扫描任务，扫描结果显示的低危漏洞个数将减少 2。
- 如果想对已忽略的漏洞恢复为风险类型，在目标漏洞所在行的“操作”列，单击“取消忽略”，恢复检测此漏洞。

步骤 8 选择“业务风险列表”页签，查看业务风险信息，如图 5-15 所示。

图5-15 风险列表

步骤 9 选择“端口列表”页签，查看目标网站的端口信息，如图 5-16 所示。

图5-16 端口列表



步骤 10 选择“站点结构”页签，查看目标网站的站点结构信息，如图 5-17 所示。

说明

站点结构显示的是目标任务的漏洞的具体站点位置，如果任务暂未扫描出漏洞，站点结构无数据显示。

显示目标网站的基本信息，包括：

- IP 地址：目标网站的 IP 地址。
- 服务器：目标网站部署所使用的服务器名称（例如：Tomcat 、Apache httpd、 IIS 等）。
- 语言：目标网站所使用的开发语言（例如：PHP、JAVA、C#等）。

图5-17 站点结构

----结束

后续处理

当您修复网站漏洞后，在扫描详情界面右侧单击“重新扫描”，重新扫描网站后，请在网站扫描详情界面查看该漏洞是否已修复。

5.6 下载网站扫描报告

操作场景

当网站扫描任务成功完成后，您可以下载任务报告，报告目前只支持 PDF 格式。

前提条件

已成功完成网站扫描任务，即目标域名的“上一次扫描结果”状态为“已完成”。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击 ☰，选择“安全 > 漏洞扫描服务”，进入漏洞扫描服务页面。

步骤 3 在“资产列表 > 网站”页签，进入下载网站扫描报告入口，如图 5-18 所示。

图5-18 进入下载网站扫描报告入口

步骤 4 单击右上角的 生成报告，生成网站扫描报告，如图 5-19 所示。

如果报告已生成，则可跳过此步。

图5-19 生成扫描报告

说明

生成的扫描报告会在 24 小时后过期。过期后，若需要下载扫描报告，请再次单击“生成报告”，重新生成扫描报告。

步骤 5 扫描报告生成完成后，单击右上角的 下载报告，将网站扫描报告下载到本地，如图 5-20 所示。

图5-20 下载扫描报告

----结束

网站漏洞扫描报告模板说明

下载扫描报告后，您可以根据扫描结果，对漏洞进行修复，报告模板主要内容说明如下：

- 概览

  查看目标网站的扫描漏洞数。

  图5-21 查看任务概览信息

- 漏洞分析概览

  统计漏洞类型及分布情况。

图5-22 漏洞类型分析

2 漏洞分析概览

2.1 扫描概览

扫描分数&漏洞个数					
91 分	总漏洞数	高危漏洞	中危漏洞	低危漏洞	提示威胁
	9	0	0	9	0

2.2 漏洞类型分布

分类	漏洞类型	检测结果
网站安全漏洞	跨站请求伪造	安全
	信息泄露	5个漏洞 查看详情
	注入攻击	安全
	其它	2个漏洞 查看详情
	路径遍历	安全
	授权问题	安全
	弱密码	安全
	跨站脚本攻击	2个漏洞 查看详情

- 服务端口列表
  查看目标网站的所有端口信息。

图5-23 网站的端口列表

3 端口列表

端口	状态	协议	服务
8,081	Open	TCP	QuickTime Streaming Server
8,080	Open	TCP	QuickTime Streaming Server | Alternative port for HTTP. See also ports 80 and 8008. | Apache Tomcat | Atlassian JIRA applications

- 漏洞根因及详情
  您可以根据修复建议修复漏洞。

图5-24 漏洞根因及详情

4.1 信息泄露

序号	漏洞名称	漏洞级别	漏洞个数
1	X-Frame-Options头配置错误	低危	2
2	X-Content-Type-Options头配置错误	低危	2
3	不安全方法	低危	1

4.1.1 X-Frame-Options头配置错误

漏洞级别 低危

漏洞简介

响应头缺少或者配置了不安全X-Frame-Options属性，可能导致点击劫持问题

修复建议

1. 配置 X-Frame-Options 2. 对于配置了已废弃的 ALLOW-FROM，原则上不推荐使用 3. 删除重复配置的 X-Frame-Options

问题URL列表

序号	影响URL	发现时间
1	http://	2023-04-20 17:25:16
2	http://	2023-04-20 17:23:24

5.7 删除域名

操作场景

该任务指导用户通过漏洞扫描服务来删除域名。

须知

域名删除后，该资产的历史扫描数据将被删除，不可恢复。

前提条件

- 已获取管理控制台的登录帐号与密码。
- 已添加域名。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击 ☰，选择“安全 > 漏洞扫描服务”，进入漏洞扫描服务页面。

步骤 3 在“资产列表 > 网站”页签，单击对应的网站信息“操作”列的“删除”。

步骤 4 进入删除域名入口，如图 5-25 所示。

图5-25 进入删除域名入口

步骤 5 在弹出的对话框中，单击“确认”，在页面右上角弹出“域名删除成功”，则说明域名删除成功。

----结束

相关操作

有关添加域名的详细操作，请参见添加域名。

6 主机扫描

6.1 添加主机

该任务指导用户通过漏洞扫描服务添加主机。

须知

漏洞扫描服务的基础版不支持主机扫描功能，如果您是基础版用户，请通过以下方式使用主机扫描功能：

- 购买专业版或企业版
- 按次购买主机扫描功能
- 按次一次性扣费，每次最多可以扫描 20 台主机。

操作场景

漏洞扫描服务支持添加 Linux 操作系统和 Windows 操作系统的主机。

- Linux 主机扫描支持主机漏洞扫描、基线检测、等保合规检测。
- Windows 主机扫描目前仅支持主机漏洞扫描。

前提条件

已获取管理控制台的登录账号与密码。

操作步骤

步骤 1 登录管理控制台。

步骤 2 选择“安全 > 漏洞扫描服务”，进入漏洞扫描服务管理控制台。

步骤 3 在左侧导航栏，选择“资产列表 > 主机”，进入主机列表入口。

步骤 4 单击“添加主机”，进入“添加主机”页面。

步骤 5 在“添加主机”页面，执行以下操作。

- 单个添加主机

  单击“添加主机”，如图 6-1 所示，参数说明如表 6-1 所示。

  图6-1 添加主机

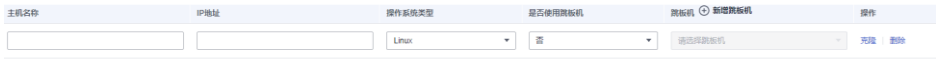


表6-1 添加主机配置参数说明

参数名称	参数说明
主机名称	用户需要添加的主机名称。
IP 地址	添加主机的公网 IP 地址。
操作系统类型	支持 Linux 操作系统和 Windows 操作系统。
是否使用跳板机	如果用户的主机需要通过代理 IP 才能访问，需要使用跳板机。 跳板机只支持 Linux 操作系统。
跳板机	可在下拉框中选择已有跳板机，或者单击“新增跳板机”，添加跳板机。
操作	• 可单击“克隆”复制主机信息。 • 可单击“删除”删除主机信息。

- 批量添加主机

  a. 单击“批量添加主机”，如图 6-2 所示，在“批量添加主机”对话框中，配置 IP 地址。多个 IP 地址，使用换行分开。

图6-2 批量添加主机

b. 单击“添加主机”。

如果需要添加新的跳板机，请执行以下操作步骤。

1. 单击“新增跳板机”。
2. 在“添加跳板机”对话框中，设置配置参数，如图 6-3 所示，配置说明如表 6-2 所示。

图6-3 添加跳板机

表6-2 跳板机配置参数说明

参数名称	参数说明
主机名称	添加的跳板机的主机名称。
公网 IP	添加的跳板机的公网 IP。
登录端口	添加的跳板机的登录端口。
选择登录方式	“密码登录”和“密钥登录”。 • 选择密码登录时，需要添加跳板机的用户名和密码。 • 选择密钥登录时，需要添加跳板机的用户名、私钥和私钥密码。
选择加密密钥	为了保护主机登录密码或密钥安全，请您必须使用加密密钥，以避免登录密码或密钥明文存储和泄露风险。 您可以选择已有的加密密钥，如果没有可选的加密密钥，请单击“创建密钥”，创建 VSS 专用的默认主密钥。

3. 单击“确认”。

步骤 6 单击“下一步”，添加主机完成，请参见配置 Linux 主机授权和配置 Windows 主机授权执行主机授权的操作。

----结束

6.2 配置主机授权

6.2.1 配置 Linux 主机授权

操作场景

该任务指导用户通过漏洞扫描服务对已添加的 Linux 主机进行扫描授权。

前提条件

- 已获取管理控制台的登录账号与密码。
- 已添加 Linux 主机。

操作步骤

步骤 1 登录管理控制台。

步骤 2 选择“安全 > 漏洞扫描服务”，进入漏洞扫描服务管理控制台。

步骤 3 在左侧导航栏，选择“资产列表 > 主机”，进入主机列表入口。

步骤 4 批量选择需要配置的主机，单击“批量操作 > 编辑”，进入批量授权入口，如图 6-4 所示。

图6-4 进入批量授权入口

说明

用户也可以单台主机授权，在目标主机所在行的“操作”列，单击“编辑”。

步骤 5 在主机授权页面，批量选择需要授权的主机，单击“批量配置授权信息”，如图 6-5 所示。

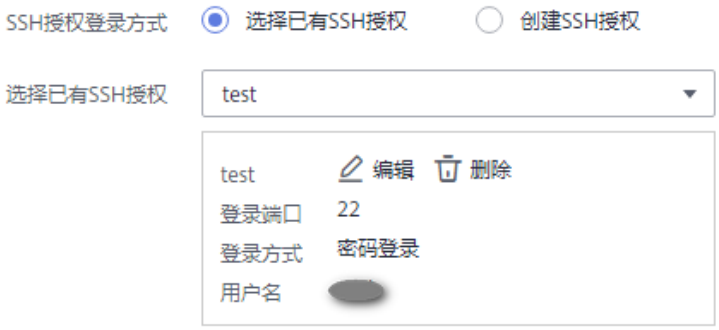
说明

- 用户也可以单台主机授权，在目标主机所在行的“操作”列，单击“配置授权信息”。
- 如果需要修改主机名称，单击，在弹出的对话框中，进行修改。

图6-5 批量授权

步骤 6 选择 SSH 授权方式进行主机授权。

图6-6 SSH 授权登录



说明

- 如果需要修改已有 SSH 授权，单击“编辑”，进行修改。
- 如果需要删除已有 SSH 授权，单击“删除”，进行删除。

选择已有 SSH 授权，或者单击“创建 SSH 授权”创建 SSH 授权，如图 6-7 所示，参数说明如表 6-3 所示。

图6-7 创建 SSH 授权

表6-3 参数说明

参数名称	参数说明
SSH 授权别称	自定义 SSH 授权名称。
登录端口	SSH 授权登录的端口号。 请确保安全组已添加该端口，以便主机可通过该端口访问 VSS。
选择登录方式	• “密码登录” • “密钥登录”
选择加密密钥	为了保护主机登录密码或密钥安全，请您必须使用加密密钥，以避免登录密码或密钥明文存储和泄露风险。 您可以选择已有的加密密钥，如果没有可选的加密密钥，请单击“创建密钥”，创建 VSS 专用的默认主密钥。
Root 权限是否加固	打开该权限后，不可以用 root 账号直接登录，而只能通过普通用户登录，然后才能切换到 root 用户。
sudo 用户名	默认为 root。
sudo 密码	设置 sudo 用户对应的密码，为了您的账号安全，您的密码会加密保存。

步骤 7 单击“确认”，完成 Linux 主机授权。

步骤 8 单击“确定”，Linux 主机授权成功。

----结束

相关操作

配置主机授权后，您可以取消主机授权，取消主机授权后，将不能完全扫描出主机的安全风险。有关取消主机授权的详细操作，请参见取消主机授权。

6.2.2 配置 Windows 主机授权

操作场景

该任务指导用户通过漏洞扫描服务对已添加的 Windows 主机进行扫描授权。

前提条件

- 已获取管理控制台的登录账号与密码。
- 登录用户只支持 Administrator。
- 已添加 Windows 主机。

操作步骤

步骤 1 登录管理控制台。

步骤 2 选择“安全 > 漏洞扫描服务”，进入漏洞扫描服务管理控制台。

步骤 3 在左侧导航栏，选择“资产列表 > 主机”，进入主机列表入口。

步骤 4 批量选择需要配置的主机，单击“批量操作 > 编辑”，进入批量授权入口，如图 6-8 所示。

图6-8 进入批量授权入口

说明

用户也可以单台主机授权，在目标主机所在行的“操作”列，单击“编辑”。

步骤 5 在主机授权页面，批量选择需要授权的主机，单击“批量配置授权信息”，如图 6-9 所示。

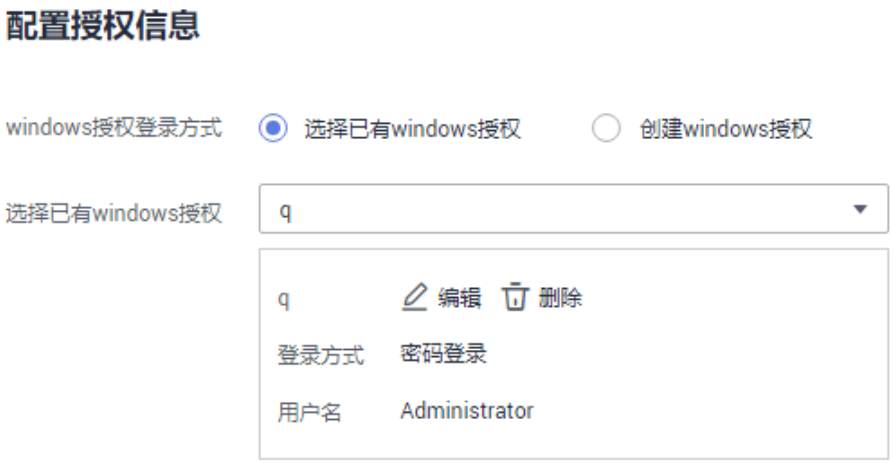
说明

- 用户也可以单台主机授权，在目标主机所在行的“操作”列，单击“配置授权信息”。
- 如果需要修改主机名称，单击，在弹出的对话框中，进行修改。

图6-9 批量授权 Windows 主机

步骤 6 在弹出的对话框中，选择已有 windows 授权，或者单击“创建 windows 授权”创建 windows 授权，如图 6-10 所示。

图6-10 配置授权信息



说明

- 如果需要修改已有 windows 授权，单击“编辑”，进行修改。
- 如果需要删除已有 windows 授权，单击“删除”，进行删除。

如果没有 windows 授权，单击“创建 windows 授权”创建授权，如图 6-11 所示，参数说明如表 6-4。

图6-11 创建 windows 授权

表6-4 参数说明

参数名称	参数说明
windows 授权别称	自定义 windows 授权名称。

参数名称	参数说明
用户名	默认为 Administrator。
密码	windows 系统登录密码。
账号域	查看该 windows 系统的账号域并填写到此处，该参数也可以为空，不填写。

步骤 7 单击“确认”，完成 Windows 主机授权。

步骤 8 单击“确定”，Windows 主机授权成功。

----结束

相关操作

配置主机授权后，您可以取消主机授权，取消主机授权后，将不能完全扫描出主机的安全风险。有关取消主机授权的详细操作，请参见取消主机授权。

Windows 主机漏洞扫描依赖于 winrm 服务开启，如何开启请参照如何开启 winrm 服务。

6.3 开启主机扫描

操作场景

该任务指导用户通过漏洞扫描服务开启主机扫描。

开启主机扫描后，漏洞扫描服务将对主机进行漏洞扫描与基线检测。

须知

漏洞扫描服务的基础版不支持主机扫描功能，如果您是基础版用户，请通过以下方式使用主机扫描功能：

- **购买专业版或企业版**
- **按次购买主机扫描功能**
- **按次一次性扣费，每次最多可以扫描 20 台主机。**

前提条件

- 已获取管理控制台的登录账号和密码。
- 已添加主机。

说明

为了确保扫描成功，在开启主机扫描前，请参照配置 Linux 主机授权和配置 Windows 主机授权完成主机授权。

开启主机扫描（专业版/企业版）

步骤 1 登录管理控制台。

步骤 2 选择“安全 > 漏洞扫描服务”，进入漏洞扫描服务管理控制台。

步骤 3 在左侧导航栏，选择“资产列表 > 主机”，进入主机列表入口。

步骤 4 单击主机信息“操作”列的“扫描”，进入主机扫描入口，如图 6-12 所示。

图6-12 进入主机扫描入口

说明

您可以选中需要扫描的主机，在主机列表上方单击“一键扫描”，对选中的多台主机批量进行扫描。

步骤 5 在弹出的对话框中，单击“确认”。

----结束

开启主机扫描（基础版）

漏洞扫描服务的基础版不支持主机扫描功能，如果您是基础版用户，请通过以下方式使用主机扫描功能：

- 购买专业版或企业版
- 按次购买主机扫描功能
- 按次一次性扣费，每次最多可以扫描 20 台主机。

请参照以下操作步骤，按需购买主机扫描功能。

步骤 1 登录管理控制台。

步骤 2 选择“安全 > 漏洞扫描服务”，进入漏洞扫描服务管理控制台。

步骤 3 在左侧导航栏，选择“资产列表 > 主机”，进入主机列表入口。

步骤 4 勾选需要扫描的主机，单击“一键扫描”，进入主机扫描入口。

步骤 5 在弹出的对话框中，选中“我已了解并同意支付该笔费用”，单击“确定”。

图6-13 “开启主机扫描”对话框

当账户余额充足时，系统在自动扣费后，将执行主机扫描任务。

须知

- 当主机扫描任务成功时，请查看主机扫描详情，详细操作请参见查看主机扫描详情。
- 当主机扫描任务失败时，请在扫描详情页面单击“重新扫描（免费）”，系统将重新执行扫描任务。

----结束

6.4 查看主机扫描详情

操作场景

该任务指导用户通过漏洞扫描服务查看主机扫描详情。

说明

- Linux 主机扫描支持主机漏洞扫描、基线检测、等保合规检测。
- Windows 主机扫描目前仅支持主机漏洞扫描。

前提条件

- 已获取管理控制台的登录账号和密码。
- 主机扫描任务已成功完成。

操作步骤

步骤 1 登录管理控制台。

步骤 2 选择“安全 > 漏洞扫描服务”，进入漏洞扫描服务管理控制台。

步骤 3 在左侧导航栏，选择“资产列表 > 主机”，进入主机列表入口。

步骤 4 查看主机信息，相关参数说明如表 6-5 所示。

表6-5 主机资产列表参数说明

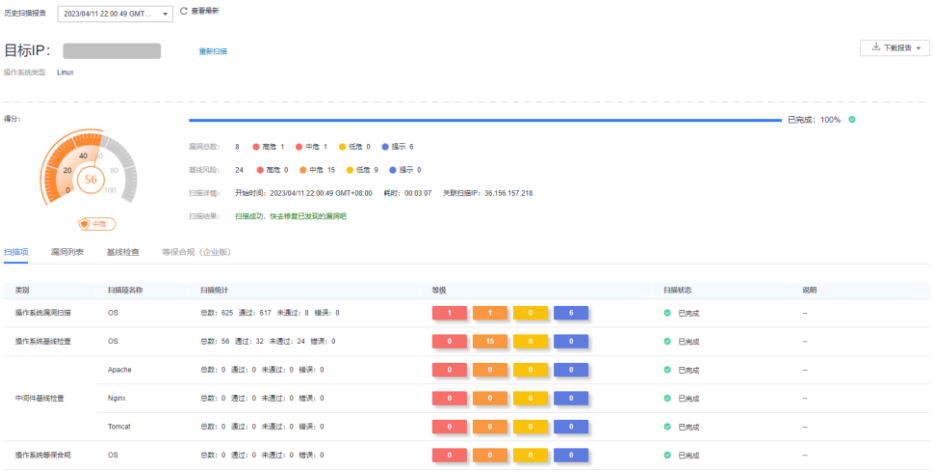
参数	参数说明
主机信息	• IP • 主机名称 • VPC
所在分组/区域/操作系统	主机所在分组/区域/操作系统，可在目标主机的“操作”列，单击“更换分组”，更换主机组。
跳板机/授权信息	• 添加跳板机的具体操作请参见添加主机。 • 主机授权的具体操作请参见配置 Linux 主机授权和配置 Windows 主机授权。
上一次扫描时间	主机最近一次扫描任务扫描时间。
上一次扫描结果	主机最近一次扫描任务的信息，包括得分和各等级的漏洞数量。单击分数或者“查看详情”，进入“任务详情”界面查看扫描概况。

步骤 5 在目标主机所在行的“上一次扫描结果”列，单击分数或者“查看详情”，查看相应任务的“扫描项总览”，如图 6-14 所示，各栏目说明如表 6-6 所示。

须知

基础版用户按次购买主机扫描功能后，如果扫描任务失败，请在扫描详情页面单击“重新扫描（免费）”，系统将重新执行扫描任务。

图6-14 查看主机扫描详情



说明

扫描任务详情界面默认显示最近一次的扫描情况，如果您需要查看其他时间的扫描情况，在“历史扫描报告”下拉框中，选择扫描时间点。

单击“查看最新”即可查看最新时间的扫描情况。

表6-6 详情总览说明

栏目	说明
目标 IP	主机 IP。
任务信息	显示目标任务的基本信息，包括： • 得分：任务被创建后，初始得分是一百分，任务扫描完成后，根据扫描出的漏洞个数和漏洞级别会扣除相应的分数，无漏洞则不扣分。 • 漏洞总数：漏洞总数及各级别的漏洞个数。 • 基线风险：各级别的基线风险个数，windows 扫描暂不支持此项检测。 • 等保合规：为您提供本地化、系统化、专业的等保测评服务，为您提供一站式安全产品及服务，帮助您测评整改，提升安全防护能力，快速满足国家实行的网络安全等级保护制度，window 扫描暂不支持此项检测。 须知 仅企业版可查看“等保合规”功能的检测结果。 • 扫描详情：开始时间及任务扫描耗时。 • 扫描结果：扫描任务的执行结果，有“扫描成功”和“扫描失败”两种结果。
扫描项	显示扫描任务的类别、扫描项名称、扫描统计、等级和扫描状态。

步骤 6　选择“扫描项”页签，查看目标主机的扫描项信息，如图 6-15 所示。

图6-15 扫描项

步骤 7　选择“漏洞列表”页签，查看目标主机的漏洞信息，如图 6-16 所示。

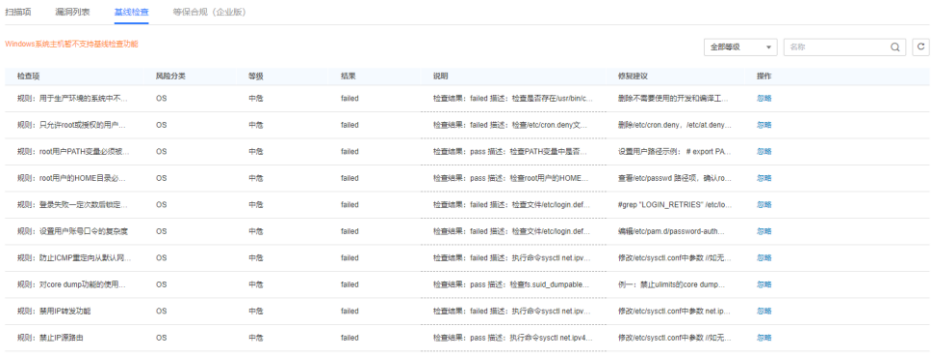
图6-16 漏洞列表界面

说明

- 如果您确认扫描出的漏洞不会对主机造成危害，您可以在目标漏洞所在行的“操作”列，单击“忽略”，忽略该漏洞，后续执行扫描任务会扫描出该漏洞，但相应的漏洞统计结果将发生变化，扫描报告中也不会出现该漏洞。
- 单击漏洞名称，进入“漏洞详情”页面，根据修复建议修复漏洞。

步骤 8　选择“基线检查”页签，查看主机扫描的基线检查信息，如图 6-17 所示。

图6-17 基线检查



说明

- 如果您确认扫描出的检查项不会对主机造成危害，您可以在目标检查项所在行的“操作”列，单击“忽略”，忽略该检查项，后续执行扫描任务会扫描出该漏洞，但相应的检查项统计结果将发生变化，扫描报告中也不会出现该检查项。
- Windows 扫描暂不支持基线检测扫描。

步骤 9 单击“等保合规（企业版）”页签，进入“等保合规（企业版）”的详情列表界面，显示目标主机的等保合规检测信息，如图 6-18 所示。

图6-18 等保合规

须知

- 如果您确认扫描出的检查项不会对主机造成危害，您可以在目标检查项所在行的“操作”列，单击“忽略”，忽略该检查项，后续执行扫描任务会扫描出该漏洞，但相应的检查项统计结果将发生变化，扫描报告中也不会出现该检查项。
- VSS 目前仅企业版用户支持等保合规检测，如果您需要对您的主机进行等保合规检测，请购买企业版。

----结束

相关操作

- 有关主机扫描得分的计算方法参考如下：

  扫描任务被创建后，初始得分是一百分，任务扫描完成后，根据扫描出的漏洞级别会扣除相应的分数。

主机扫描：高危每个减 3 分，中危每个减 2 分，低危每个减 1 分。每类漏洞最多计算 20 个。

说明

- 得分越高，表示漏洞数量越少，主机越安全。
- 如果得分偏低，请根据实际情况对漏洞进行忽略标记，或根据修复建议修复漏洞。
- 漏洞修复后，建议重新扫描一次查看修复效果。

- 有关修复主机漏洞的详细介绍，请参见《漏洞扫描服务常见问题》中“如何修复扫描出来的主机漏洞？”。

6.5 下载主机扫描报告

操作场景

当主机扫描任务成功完成后，您可以下载漏洞扫描报告和等保合规配置报告，报告目前支持 PDF 格式和 Excel 格式。

须知

VSS 目前仅企业版用户支持等保合规检测，如果您需要下载等保合规配置报告，请购买企业版。

前提条件

已成功完成主机扫描任务，即目标主机的“上一次扫描结果”状态为“已完成”。

操作步骤

步骤 1 登录管理控制台。

步骤 2 选择“安全 > 漏洞扫描服务”，进入漏洞扫描服务管理控制台。

步骤 3 在左侧导航栏，选择“资产列表 > 主机”，进入主机列表入口。

步骤 4 选择主机，单击“下载报告”，选择需要下载的报告类型，即可下载报告，如图 6-19 所示。

图6-19 下载主机扫描报告

----结束

主机漏洞扫描报告模板说明

下载扫描报告后，您可以根据扫描结果，对漏洞进行修复，报告模板说明如下：

- 概览

  查看目标主机的扫描总览信息。

  图6-20 查看扫描概览信息

  1. 概览

  扫描分数

  12分

总计	高危	中危	低危	提示
35	20	14	0	1

类别	扫描项名称	漏洞总数	等级
操作系统漏洞扫描	OS	25	16 8 0 1
操作系统基线检查	OS	10	4 6 0 0
中间件基线检查	Apache	0	0 0 0 0
	Tomcat	0	0 0 0 0
	Nginx	0	0 0 0 0

- 系统漏洞扫描详情

  您可以根据修复建议修复系统漏洞。

图6-21 查看漏洞详情以及修复建议

漏洞名称	CESA-2019:2304
漏洞等级	中危
漏洞简介	An update for openssl is now available for Red Hat Enterprise Linux 7. Red Hat Product Security has rated this update as having a security impact of Moderate. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section.
修复建议	update openssl,openssl-libs to the latest version
相关CVE	CVE-2018-0734 CVE-2019-1559

- 基线检查详情

  您可以根据修复建议修复基线漏洞。

图6-22 查看基线检查结果以及修复建议

检查项	禁止Control-Alt-Delete重启动机器命令 (Forbid_Control_Alt_Delete_Restart)
风险分类	OS
等级	中危
结果	未通过
检查说明	**子检查项:**检查/usr/lib/systemd/system/reboot.target 文件是否不存在,是否被注释完,是否为空:cat /usr/lib/systemd/system/reboot.target 2>/dev/null | grep -v "^\s*#" 2>/dev/null **检查结果:** 未通过 **子检查项:**检查是否存在软链接文件/usr/lib/systemd/system/ctrl-alt-del.target:ls /usr/lib/systemd/system/ctrl-alt-del.target 2>/dev/null **检查结果:** 未通过
修复建议	删掉/usr/lib/systemd/system/reboot.target 文件

等保合规配置报告模板说明

下载扫描报告后，您可以根据扫描结果，对漏洞进行修复，报告模板说明如下：

- 概览

  查看等保合规配置报告的概览信息。

图6-23 查看等保合规概览信息

1. 概览

- 等保合规检查详情

您可以根据修复建议修复等保合规漏洞。

图6-24 查看等保合规检查详情

2. 等保合规检查详情

检查项	更改主机解析地址的顺序
权重	1
结果	未通过
检查说明	子检查项:检查文件中是否存在order hosts，bind：egrep -v "^\s*#" /etc/host.conf | egrep -i "^\s*order\s*hosts\s*" | egrep -i bind 检查结果: 未通过 子检查项:检查文件中是否存在multi on：egrep -v "^\s*#" /etc/host.conf | egrep -i "^\s*multi\s*on\s*" 检查结果: 通过 子检查项:检查文件中是否存在nospoof on：egrep -v "^\s*#" /etc/host.conf | egrep -i "^\s*nospoof\s*on\s*" 检查结果: 未通过
修复建议	在文件/etc/host.conf中修改或添加如下内容： order hosts，bind multi on nospoof on

表3.1 更改主机解析地址的顺序

6.6 其他操作

6.6.1 添加跳板机

操作场景

该任务指导用户通过漏洞扫描服务为 Linux 系统的主机配置跳板机。

说明

当前仅支持添加 Linux 系统跳板机。

前提条件

- 已获取管理控制台的登录账号和密码。
- 已添加 Linux 系统的主机。

操作步骤

步骤 1 登录管理控制台。

步骤 2 选择“安全 > 漏洞扫描服务”，进入漏洞扫描服务管理控制台。

步骤 3 在左侧导航栏，选择“资产列表 > 主机”，进入主机列表入口。

步骤 4 批量选择需要配置的主机，单击“批量操作 > 编辑”，进入批量授权入口，如图 6-25 所示。

图6-25 进入批量授权入口

说明

用户也可以单台主机授权，在目标主机所在行的“操作”列，单击“编辑”。

步骤 5 在主机授权页面，批量选择需要添加跳板机的主机，单击“批量配置跳板机”，如图6-26 所示。

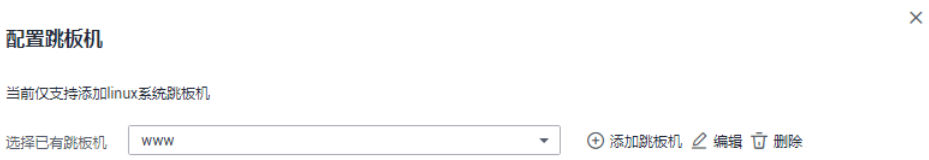
说明

- 用户也可以单台主机添加跳板机，在目标主机所在行的“操作”列，单击“配置跳板机”。
- 如果需要修改主机名称，单击，在弹出的对话框中，进行修改。

图6-26 批量配置跳板机

步骤 6 在“配置跳板机”对话框中，选择已有跳板机，或者单击“添加新的跳板机”，添加跳板机，如图 6-27 所示。

图6-27 配置跳板机



说明

- 如果需要修改已有跳板机，单击“编辑”，进行修改。
- 如果需要删除已有跳板机，单击“删除”，删除跳板机。

如果需要添加新的跳板机，请执行以下操作步骤。

1. 单击“新增跳板机”。

2. 在“添加跳板机”对话框中，设置配置参数，如图 6-28 所示，配置说明如表 6-7 所示。

图6-28 添加跳板机

表6-7 跳板机配置参数说明

参数名称	参数说明
主机名称	添加的跳板机的主机名称。
公网 IP	添加的跳板机的公网 IP。
登录端口	添加的跳板机的登录端口。
选择登录方式	“密码登录”和“密钥登录”。 • 选择密码登录时，需要添加跳板机的用户名和密码。 • 选择密钥登录时，需要添加跳板机的用户名、私钥和私钥密码。
选择加密密钥	为了保护主机登录密码或密钥安全，请您必须使用加密密钥，以避免登录密码或密钥明文存储和泄露风险。 您可以选择已有的加密密钥，如果没有可选的加密密钥，请单击“创建密钥”，创建 VSS 专用的默认主密钥。

3. 单击“确认”。

步骤 7 单击“确定”，跳板机配置成功。

如果需要解除绑定主机的跳板机，在目标主机的“操作”列，单击“更多 > 解除跳板机”，解除跳板机。

----结束

6.6.2 取消主机授权

操作场景

该任务指导用户通过漏洞扫描服务取消主机授权。

取消主机授权后，将不能完全扫描出主机的安全风险，请谨慎操作。

前提条件

- 已获取管理控制台的登录账号与密码。
- 已添加主机。
- 已开通预置账号。
- 已在创建任务时授权通过网络连接到对应的主机，即已进行主机授权。

操作步骤

步骤 1 登录管理控制台。

步骤 2 选择“安全 > 漏洞扫描服务”，进入漏洞扫描服务管理控制台。

步骤 3 在左侧导航栏，选择“资产列表 > 主机”，进入主机列表入口。

步骤 4 批量选择需要配置的主机，单击“批量操作 > 编辑”，进入批量授权入口，如图 6-29 所示。

图6-29 进入批量授权入口

说明

用户也可以单台主机授权，在目标主机所在行的“操作”列，单击“编辑”。

步骤 5 在目标主机的“操作”列，单击“更多”，在下拉框中，单击“解除授权”，如图 6-30 所示。

解除授权后，“授权信息”的状态为“暂未配置”。

图6-30 解除授权

步骤 6 单击“确定”，解除授权成功。

----结束

6.6.3 更换分组

操作场景

该任务指导用户通过漏洞扫描服务为已添加的主机更换分组。

前提条件

- 已获取管理控制台的登录账号和密码。
- 已添加主机。

操作步骤

步骤 1 登录管理控制台。

步骤 2 选择“安全 > 漏洞扫描服务”，进入漏洞扫描服务管理控制台。

步骤 3 在左侧导航栏，选择“资产列表 > 主机”，进入主机列表入口。

步骤 4 在目标主机的操作列，单击“更换分组”。

- 在已有“主机组”下拉列表中，选择已有的主机组，如图 6-31 所示。

图6-31 更换分组

- 单击“新建分组”页签，输入“主机组名称”，创建新的主机组，如图 6-32 所示。

图6-32 新建分组

步骤 5 单击“确认”，主机更换分组成功。

说明

用户可以同时更换多个主机的分组。选中多个主机后，单击“批量操作 > 更换分组”，在弹出的对话框中，重新设置主机组名称，单击“确定”，批量变更分组。

----结束

6.6.4 删除主机

操作场景

该任务指导用户通过漏洞扫描服务删除已添加的主机。

删除主机后，该主机的所有扫描历史报告将会被删除，请谨慎操作。

前提条件

- 已获取管理控制台的登录账号和密码。
- 已添加主机。

操作步骤

步骤 1 登录管理控制台。

步骤 2 选择“安全 > 漏洞扫描服务”，进入漏洞扫描服务管理控制台。

步骤 3 在左侧导航栏，选择“资产列表 > 主机”，进入主机列表入口。

步骤 4 在目标主机的“操作”列，单击“删除”，在弹出的对话框中，单击“确定”。

说明

用户可以同时删除多个主机。选中多个主机后，单击“批量操作 > 删除”，在弹出的对话框单击“确定”，批量删除主机。

----结束

7 安全监测

7.1 新增监测任务

操作场景

漏洞扫描服务支持网站扫描，网站是您的“资产”，您可以在“安全监测”界面对您的资产进行安全扫描与编辑操作。

该任务指导用户通过漏洞扫描服务新增监测任务，监测任务新增成功后，自动开启监测。

须知

漏洞扫描服务的基础版不支持安全监测功能，如果您是基础版用户，请您通过购买专业版、高级版或企业版使用该功能。

前提条件

- 已获取管理控制台的登录帐号与密码。
- 域名的“认证状态”为“已认证”。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击 ☰，选择“安全 > 漏洞扫描服务”，进入漏洞扫描服务页面。

步骤 3 在“安全监测”页面，单击“新增监测任务”。

步骤 4 进入新增监测任务入口，如图 7-1 所示。

图7-1 进入新增监测任务

步骤 5 在“新增监测任务”界面，请根据表 7-1 进行扫描设置，设置后如图 7-2 所示。

图7-2 监测任务的扫描设置

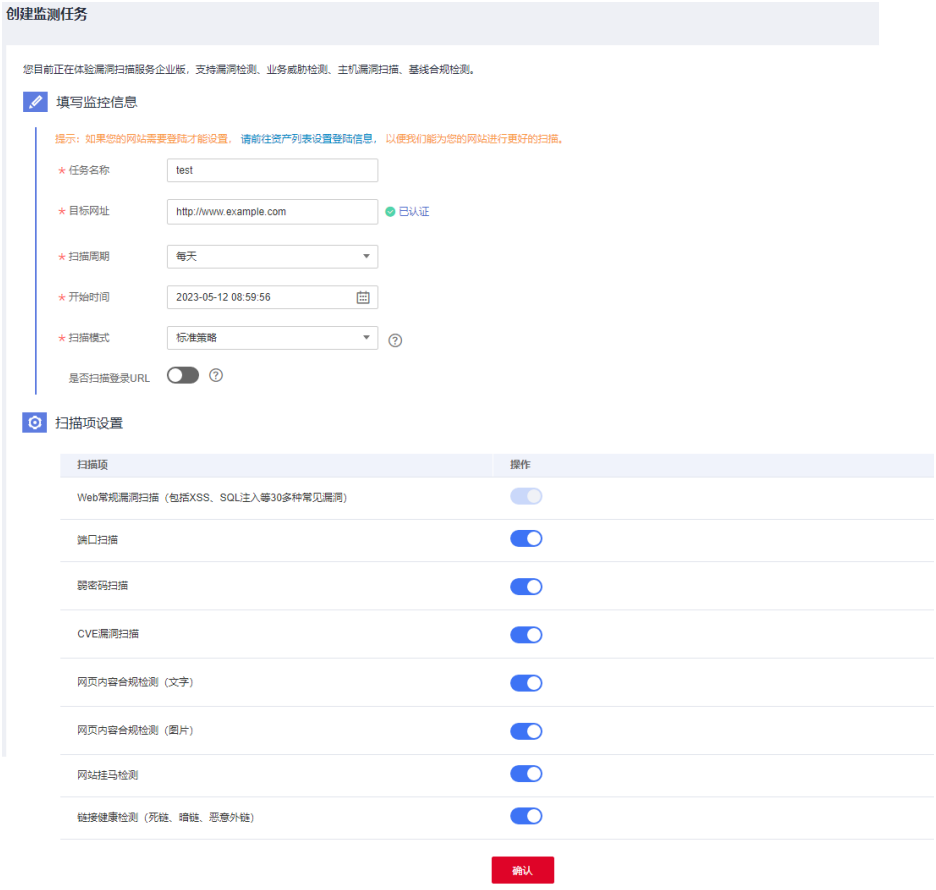


表7-1 扫描设置参数说明

参数	参数说明
任务名称	用户自定义。
目标网址	待扫描的网站地址或 IP 地址。 通过下拉框选择已认证通过的域名。
扫描周期	单击下拉框选择任务扫描周期。 • 每天

参数	参数说明
	• 每三天 • 每周 • 每月
开始时间	设置监测任务开始的时间。
扫描模式	三种扫描模式： • 极速策略：扫描耗时最少，能检测到的漏洞相对较少。 • 标准策略：扫描耗时适中，能检测到的漏洞相对较多。 • 深度策略：扫描耗时最长，能检测到最深处的漏洞。
是否扫描登录 URL	默认不扫描登录 URL，开启扫描登录 URL 前，请务必确认不会影响正常业务
扫描项设置	VSS 支持的扫描项参照表 7-2。 •  ：开启 •  ：关闭

表7-2 扫描项设置

扫描项名称	说明
Web 常规漏洞扫描（包括 XSS、SQL 注入等 30 多种常见漏洞）	提供了常规的 30 多种常见漏洞的扫描，如 XSS、SQL 等漏洞的扫描。默认为开启状态，不支持关闭。
端口扫描	检测主机打开的所有端口。
弱密码扫描	对网站的弱密码进行扫描检测。
CVE 漏洞扫描	CVE，即公共暴露漏洞库。VSS 可以快速更新漏洞规则，扫描最新漏洞。
网页内容合规检测（文字）	对网站文字的合规性进行检测。
网页内容合规检测（图片）	对网站图片的合规性进行检测。
网站挂马检测	挂马：上传木马到网站上，使得网站在运行的时候执行木马程序，被黑客控制，遭受损失。VSS 可以检测网站是否存在挂马。
链接健康检测（死链、暗链、恶意外链）	对网站的链接地址进行健康性检测，避免您的网站出现死链、暗链、恶意链接。

步骤 6 设置完成后，单击“确认”。

----结束

7.2 暂停监测任务

操作场景

该任务指导用户通过漏洞扫描服务停止资产的监测。

前提条件

- 已获取管理控制台的登录帐号与密码。
- 已开启资产的监测任务。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击 ，选择“安全 > 漏洞扫描服务”。

步骤 3 在左侧导航树中，选择“安全监测”，进入“安全监测”界面，如图 7-3 所示。

图7-3 监测列表

步骤 4 在目标监测任务所在行的“操作”列中，单击“暂停监测”，在弹出的对话框中，单击“确认”。

说明

如果用户需要再次开启监测任务，在目标监测任务所在行的“操作”列中，单击“开启监测”，开启监测任务。

----结束

7.3 编辑监测任务

操作场景

该任务指导用户通过漏洞扫描服务编辑资产的监测任务。

前提条件

- 已获取管理控制台的登录帐号与密码。
- 已创建监测任务。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击 ☰，选择“安全 > 漏洞扫描服务”。

步骤 3 在左侧导航树中，选择“安全监测”，进入“安全监测”界面，如图 7-4 所示。

图7-4 监测列表页面

步骤 4 在目标监测任务所在行的“操作”列中，单击“编辑任务”，如图 7-5 所示。

图7-5 编辑监测任务

步骤 5　根据需求，重新配置监控信息和扫描项设置。

----结束

7.4 删除监测任务

操作场景

该任务指导用户通过漏洞扫描服务删除已创建的监测任务。

前提条件

- 已获取管理控制台的登录帐号与密码。
- 已创建监测任务。

操作步骤

步骤 1　登录管理控制台。

步骤 2 在左侧导航树中，单击 ☰，选择“安全 > 漏洞扫描服务”。

步骤 3 在左侧导航树中，选择“安全监测”，进入“安全监测”界面，如图 7-6 所示。

图7-6 监测列表信息

步骤 4 在目标监测任务所在行的“操作”列中，单击“删除任务”，在弹出的对话框中，单击“确认”。

----结束

7.5 查看安全监测列表

操作场景

该任务指导用户通过漏洞扫描服务查看安全监测列表。

前提条件

- 已获取管理控制台的登录帐号与密码。
- 已新增监测任务。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击 ☰，选择“安全 > 漏洞扫描服务”，

步骤 3 在左侧导航树中，选择“安全监测”，进入“安全监测”界面，如图 7-7 所示，相关参数说明如表 7-3 所示。

图7-7 查看安全监测列表

表7-3 安全监测列表参数说明

参数	参数说明
任务名称	创建监测任务时用户自定义的任务名称。
监测周期	监测任务开始执行的周期。 • 每天 • 每三天 • 每周 • 每月
监测资产	创建监测任务时填写的目标网址。
扫描模式	扫描模式分为“极速策略”、“标准策略”和“深度策略”，建议选择“深度策略”模式。
扫描开始时间	最近一次扫描开始的时间。
最近一次扫描情况	最近一次扫描任务的信息，包括得分和各等级的漏洞数量。单击*分数*或者“查看详情”，进入“扫描详情”界面查看扫描概况。

----结束

7.6 查看任务详情

操作场景

该任务指导用户通过漏洞扫描服务查看任务详情。

前提条件

- 已获取管理控制台的登录帐号与密码。
- 已开启了资产的监测任务。

操作步骤

步骤 1 登录管理控制台。

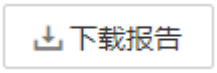
步骤 2 在左侧导航树中，单击 ☰，选择“安全 > 漏洞扫描服务”。

步骤 3 在左侧导航树中，选择“安全监测”，进入“安全监测”界面，如图 7-8 所示。

图7-8 安全监测列表

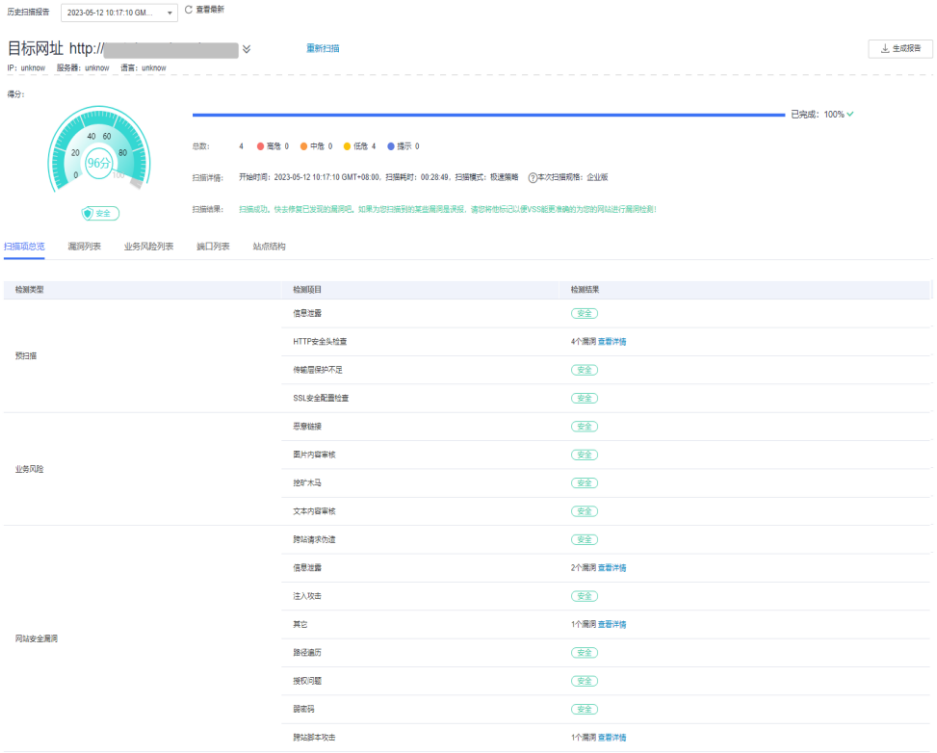
步骤 4 在目标监测任务所在行的“最近一次扫描情况”列，单击*分数*或者“查看详情”，进入“任务详情”界面，可以查看相应任务的“扫描项总览”，如图 7-9 所示。

说明

- 扫描任务详情界面默认显示最近一次的扫描情况，如果您需要查看其他时间的扫描情况，在“历史扫描报告”下拉框中，选择扫描时间点。
- 单击“重新扫描”，可以重新执行扫描任务。
- 当扫描任务成功完成后，单击右上角的“生成报告”，生成网站扫描报告后，单击右上角的 

，可以下载任务报告，目前只支持 PDF 格式。

图7-9 查看扫描详情



步骤 5 选择“扫描项总览”页签，查看扫描项的检测结果，如图 7-10 所示。

图7-10 扫描项总览

说明

如果检测结果存在漏洞或者风险，可在“检测结果”列，单击“查看详情”了解漏洞或者风险的详细情况。

步骤 6 选择“漏洞列表”页签，查看漏洞信息，如图 7-11 所示。

图7-11 漏洞列表

说明

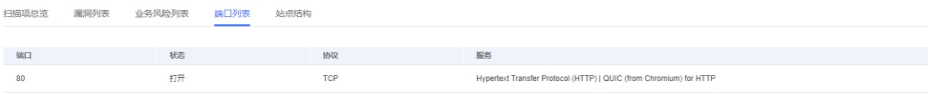
- 单击“查看更多”，可以查看详细的漏洞分析。
- 单击漏洞名称可以查看相应漏洞的“漏洞详情”、“漏洞简介”、“修复建议”。
- 如果您确认扫描出的漏洞不会对网站造成危害，请在目标漏洞所在行的“操作”列，单击“忽略”，忽略该漏洞，后续执行扫描任务会扫描出该漏洞，但扫描结果将不会统计忽略的漏洞。例如，如果您对 2 个低危漏洞执行了“忽略”操作，则再次执行扫描任务，扫描结果显示的低危漏洞个数将减少 2。
- 如果想对已忽略的漏洞恢复为风险类型，在目标漏洞所在行的“操作”列，单击“取消忽略”，恢复检测此漏洞。

步骤 7 选择“业务风险列表”页签，查看业务风险信息，如图 7-12 所示。

图7-12 风险列表

步骤 8 选择“端口列表”页签，查看目标网站的端口信息，如图 7-13 所示。

图7-13 端口列表



步骤 9 选择“站点结构”页签，查看目标网站的站点结构信息，如图 7-14 所示。

说明

站点结构显示的是目标任务的漏洞的具体站点位置，如果任务暂未扫描出漏洞，站点结构无数据显示。

显示目标网站的基本信息，包括：

- IP 地址：目标网站的 IP 地址。
- 服务器：目标网站部署所使用的服务器名称（例如：Tomcat 、Apache httpd、 IIS 等）。
- 语言：目标网站所使用的开发语言（例如：PHP、JAVA、C#等）。

图7-14 站点结构信息

----结束

8 总览

操作场景

该任务指导用户通过“总览”查看网站和主机扫描概况，主要展示资产信息、最近一次扫描情况和最近扫描任务列表信息。

前提条件

- 已获取管理控制台的登录帐号与密码。
- 已添加网站和主机。

查看扫描概况

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击 ☰，选择“安全 > 漏洞扫描服务”，进入“总览”界面。

步骤 3 查看扫描概况。

- 查看资产信息，如图 8-1 所示，资产信息参数说明如表 8-1 所示。

图8-1 资产信息

表8-1 资产信息参数说明

参数	说明	操作
网站数量	显示网站、已认证、未认证的网站个数。	单击网站总个数可以进入到相应的资产列表。

参数	说明	操作
	说明 当网站的个数为 0 时，单击“添加资产”，进入到资产列表界面添加网站。	
主机数量	显示主机、已授权、未授权的主机个数。 说明 当主机的个数为 0 时，单击“添加资产”，进入到资产列表界面添加主机。	单击主机总个数可以进入到相应的资产列表。
网站风险统计	统计所有网站的风险详情。	--
主机风险统计	统计所有主机的风险详情。	--
最危险网站	• 得分最低的网站为最危险的网站，如果得分一样，则比较高危漏洞个数、中危漏洞个数.....依次类推。 • 如果用户添加了网站且所有网站的扫描得分是 100 分，则没有最危险网站，展示“--”。 • 显示网站不同等级的风险个数。	• 单击最危险网站，可以进入到该网站的最近一次扫描任务详情。 • 风险等级有：高危、中危、低危和提示。
最危险主机	• 得分最低的主机为最危险的主机，如果得分一样，则比较高危漏洞个数、中危漏洞个数.....依次类推。 • 如果用户添加了主机且所有主机的扫描得分是 100 分，则没有最危险主机，展示“--”。 • 显示主机不同等级的风险个数。	• 单击最危险主机，可以进入到该主机的最近一次扫描任务详情。 • 风险等级有：高危、中危、低危和提示。

- 最近一次扫描情况，如图 8-2 所示，参数说明如表 8-2 说明。
  单击切换按钮，可查看最近一次扫描的网站或主机结果信息。

  图8-2 最近一次扫描情况

说明

- 当扫描未完成的时候，不展示分数，而是展示扫描状态，未完成的扫描状态有“等待中”、“进行中”。
- 如果扫描任务是失败的，则展示上一次扫描成功的任务详情。

表8-2 扫描情况参数说明

参数	说明	操作
扫描对象	扫描的网站和主机。	单击网站或主机可进入本次任务的扫描详情。
开始时间	开始扫描的时间。	--
扫描耗时	扫描全过程所耗的时间。	--
任务状态	• 已完成 • 进行中 • 等待中	--
漏洞总数	显示网站不同等级的风险个数。	风险等级有：高危、中危、低危、和提示。
TOP 风险	根据扫描项的漏洞数量排序而来。	--

- 最近扫描任务列表，如图 8-3 所示，参数说明如表 8-3 说明。

图8-3 最近扫描任务列表

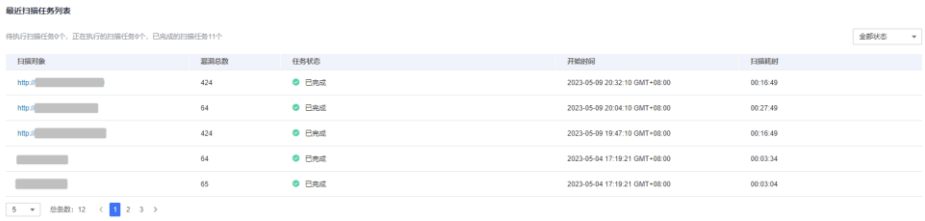


表8-3 任务列表参数说明

参数	说明	操作
扫描对象	扫描的网站和主机。	单击网站和主机可进入本次任务的扫描详情。
漏洞总数	显示网站和主机的风险漏洞总数。	--

参数	说明	操作
任务状态	三个状态：“等待中”、“进行中”、“已完成”。	--
开始时间	开始扫描的时间。	--
扫描耗时	扫描全过程所耗的时间。	--

----结束

9 最佳实践

9.1 扫描具有复杂访问机制的网站漏洞

场景说明

如果您的网站“www.example.com”除了需要账号密码登录，还有其他的访问机制（例如，需要输入动态验证码），请您设置“cookie 登录”方式进行网站漏洞扫描，以便 VSS 能为您发现更多安全问题。

在添加域名并完成域名认证后，请您参照本文档对具有复杂访问机制的网站（“www.example.com”）进行漏洞扫描，操作流程如下：

①获取网站的 cookie 值 → ②设置网站“cookie 登录”方式 → ③创建扫描任务 → ④查看扫描结果并下载扫描报告

步骤 1：获取网站的 cookie 值

须知

为了确保获取的 cookie 值有效，请您在获取 cookie 值后保持网页的登录状态，再执行步骤 2：设置网站 cookie 登录方式～步骤 4：查看扫描结果并下载扫描报告。

以 Google Chrome 浏览器为例说明，获取网站的 cookie 值的步骤如下：

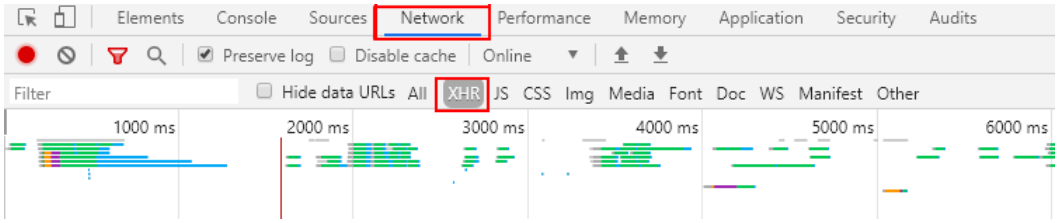
步骤 1 打开 Google Chrome 浏览器。

步骤 2 按“F12”，进入浏览器的开发者模式。

步骤 3 在地址栏中输入目标网站地址“www.example.com”。

步骤 4 在调试页面中，选择“Network > XHR” ，如图 9-1 所示。

图9-1 Network 页面



步骤 5 在左侧导航树中，选择一个 http 请求。

步骤 6 在“Headers”页面的“Request Headers”区域框，获取当前网站页面的“Cookie”字段值，如图 9-2 所示。

图9-2 获取 cookie 值

----结束

步骤 2：设置网站“cookie 登录”方式

请参照以下操作步骤设置“cookie 登录”方式。

步骤 1 登录管理控制台。

步骤 2 进入网站登录设置入口，如图 9-3 所示。

图9-3 进入网站登录设置入口

步骤 3 在弹出的“编辑”对话框中，将图 9-2 中网站的 cookie 值完整复制到“cookie 值”文本框中。

图9-4 设置 cookie 登录方式

步骤 4 在“验证登录网址”文本框中输入用于验证登录的网址。

输入登录成功后才能访问的网址，便于 VSS 快速判断您的登录信息是否有效。

步骤 5 单击“确认”，完成网站登录设置。

----结束

步骤 3：创建扫描任务

须知

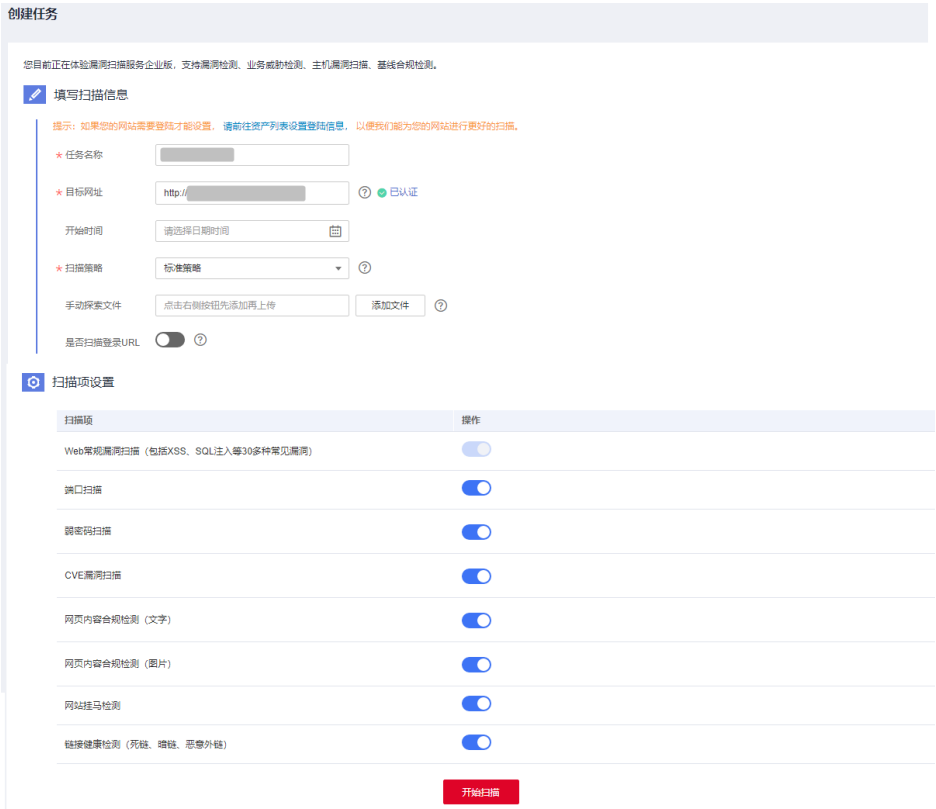
创建扫描任务时，请您保持网站的登录状态，以免 cookie 失效。

步骤 1 在该域名所在行的“操作”列，单击“扫描”，如图 9-5 所示。

图9-5 创建扫描任务

步骤 2 在“创建任务”界面，根据扫描需求，设置扫描参数，如图 9-6 所示。

图9-6 创建扫描任务



步骤 3 单击“开始扫描”。

如果没有设置开始扫描时间，且此时服务器没有被占用，则创建的任务可立即开始扫描，任务状态为“进行中”；否则进入等待队列中等待，任务状态为“等待中”。

----结束

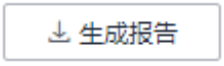
步骤 4：查看扫描结果并下载扫描报告

扫描任务执行成功（域名的“上一次扫描结果”状态为“已完成”），您可以查看扫描结果并下载扫描报告。

步骤 1 在该域名所在行的“上一次扫描结果”列，单击扫描得分。

步骤 2 在扫描任务详情界面，查看扫描结果，如图 9-7 所示。

图9-7 查看扫描任务详情

步骤 3 单击右上角的 

，生成网站扫描报告。

如果报告已生成，则可跳过此步。

步骤 4 单击右上角的 

，将网站扫描报告下载到本地，查看详细的扫描结果。

报告目前只支持 PDF 格式。

----结束

10 常见问题

10.1 产品咨询类

10.1.1 漏洞扫描服务的扫描 IP 有哪些？

如果您的网站设置了防火墙或其他安全策略，将导致 VSS 的扫描 IP 被当成恶意攻击者而误拦截。因此，在使用 VSS 前，请您将以下 VSS 的扫描 IP 添加至网站访问的白名单中：

114.217.39.79，222.93.127.109

说明

VSS 会模拟客户端使用随机端口连接被测试设备，建议放通来自 vss 这些 ip 的全量端口。

10.1.2 漏洞扫描服务可以免费使用吗？

漏洞扫描服务提供了基础版、专业版、高级版和企业版四种服务版本。其中，基础版配额内的服务免费，部分功能按需计费；专业版、高级版和企业版需要收费。

基础版配额内提供的网站漏洞扫描服务（域名个数：5 个，扫描次数：每日 5 次）是免费的。

有关 VSS 收费的详细介绍，请参见漏洞扫描服务如何收费？ 。

10.1.3 扫描任务有哪些状态？

扫描任务的状态如表 10-1 所示。

表10-1 扫描任务状态

状态	含义
已完成	扫描完成。
进行中	正在进行扫描。
等待中	任务正在等待执行 。 说明

状态	含义
	如果没有设置开始扫描时间，且此时服务器没有被占用，则创建的任务可立即开始扫描，任务状态为“进行中”；否则进入等待队列中等待，任务状态为“等待中”。
已取消	任务被取消。 说明 任务在“进行中”或“等待中”才可以被取消。

任务可能经历的状态历程。

- 等待中→进行中→已完成
- 等待中→已取消
- 等待中→进行中→已取消

10.1.4 漏洞扫描服务到期后还能继续使用吗？

漏洞扫描服务到期后，可以继续使用基础版的所有功能。

10.1.5 扫描任务的得分是如何计算的？

扫描任务被创建后，初始得分是一百分，任务扫描完成后，根据扫描出的漏洞级别会扣除相应的分数。

网站扫描：

- 高危漏洞，一个扣 10 分，最多扣 60 分（6 个）。
- 中危漏洞， 一个扣 3 分，最多扣 45 分（15 个）。
- 低危漏洞， 一个扣 1 分，最多扣 30 分（30 个）。
- 无漏洞或提示漏洞不扣分。
- 扫描分数最低为 10 分。

说明

- 得分越高，表示漏洞数量越少，网站越安全。
- 如果得分偏低，请根据实际情况对漏洞进行忽略标记，或根据修复建议修复漏洞，或使用 Web 应用防火墙服务为您的网站保驾护航。
- 漏洞修复后，建议重新扫描一次查看修复效果。

10.1.6 按需计费扫描失败怎么办？

用户选择“按需计费”的方式，在进行扫描时，如果扫描任务失败，不会扣费。在解决失败问题后，如配置网站 WAF 白名单、修改扫描配置等，用户可以重新发起按需扫描，扫描成功后才会扣费。

10.1.7 漏洞扫描服务能修复扫描出来的漏洞吗？

不能。漏洞扫描服务是一款漏洞扫描工具，能为您发现您的资产存在的漏洞，不能进行资产漏洞修复，但漏洞扫描服务会为您提供详细的扫描结果以及修复建议，请您自行选择修复方法进行修复。

10.1.8 漏洞扫描服务和传统的漏洞扫描器有什么区别？

VSS 和传统的漏洞扫描器的区别如表 10-2 所示。

表10-2 VSS 和传统的漏洞扫描器的区别

对比项	传统的漏洞扫描器	VSS
使用方法	使用前需要安装客户端。	不需要安装客户端，在管理控制台创建任务（输入域名或 IP 地址）就可以进行漏洞扫描，节约运维成本。
更新漏洞库方式	手动更新漏洞库，更新不及时。	云端同步更新漏洞库，涵盖最新漏洞，可以及时检测用户的网站是否有最新爆发的漏洞威胁。

10.1.9 漏洞扫描服务支持扫描哪些漏洞？

漏洞扫描服务支持扫描的漏洞有：

- 前端漏洞

  SQL 注入、XSS、CSRF、URL 跳转等。
- 信息泄露

  端口暴露，目录遍历，备份文件，不安全文件，不安全 HTTP 方法，不安全端口。
- Web 注入漏洞

  命令注入，代码注入，XPATH 注入，SSRF 注入，反序列化等注入漏洞。
- 文件包含漏洞

  任意文件读取、任意文件包含、任意文件上传、XXE。

10.1.10 如何查看漏洞修复建议？

网站扫描查看漏洞修复建议的方法。

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击 ☰，选择“安全 > 漏洞扫描服务”，进入漏洞扫描服务页面。

步骤 3 在“资产列表 > 网站”页签，进入网站列表入口。

步骤 4 查看网站资产列表，相关参数说明如表 10-3 所示。

表10-3 网站资产列表参数说明

参数	参数说明
域名信息	• 域名/IP 地址 • 域名别称
认证状态	• “已认证” 目标域名已完成域名认证。 • “未认证” 目标域名未完成域名认证。单击“去认证”进行域名认证。
上次扫描时间	域名最近一次扫描任务的时间。
上一次扫描结果	域名最近一次扫描结果信息，包括得分和各等级的漏洞数量。单击得分或者“查看详情”，进入“扫描详情”界面查看扫描概况。

步骤 5 在目标域名所在行的“上一次扫描结果”列，单击分数或者“查看详情”，查看扫描任务详情。

步骤 6 选择“漏洞列表”页签，查看漏洞信息，如图 10-1 所示。

图10-1 漏洞列表

步骤 7 单击漏洞名称，查看相应漏洞的“漏洞详情”、“漏洞简介”、“修复建议”，如图 10-2 所示，用户可以根据修复建议修复漏洞。

图10-2 网站漏洞详情

----结束

10.1.11 使用漏洞扫描服务前需要备份数据吗？

不需要。漏洞扫描服务是无侵入式的服务，不需要备份数据。

10.1.12 漏洞扫描服务如何判定 SQL 注入风险？

对于存在运算或判断等表达式的请求，当扫描结果与原请求相似度大于 90%时，VSS 就会判定存在 SQL 注入风险。

10.1.13 漏洞扫描服务支持扫描 SQL 注入吗？

漏洞扫描服务支持扫描前端漏洞（SQL 注入、XSS、CSRF、URL 跳转等）。

10.2 网站扫描类

10.2.1 如何快速发现网站漏洞？

漏洞扫描的原理是，通过爬虫获取用户网站的 URL 列表，然后对列表中所有 URL 进行扫描。

如果用户需要快速扫描，可以在创建扫描任务时，“扫描策略”选择“极速策略”，如图 10-3 所示。

说明

扫描策略分为：极速策略、标准策略、深度策略。选择深度扫描可以更深层次的发现漏洞，建议您优先选择“深度策略”。

图10-3 设置扫描模式

10.2.2 如果网站登录需要动态验证码可以使用 VSS 的自动登录功能吗？

可以。只需要用户在网站登录设置页面配置网站的 Cookie 值，如何配置网站的 Cookie 值请参见为什么扫描任务自动登录失败了？。

10.2.3 为什么扫描任务自动登录失败了？

漏洞扫描服务在扫描过程中，会在用户提交的登录页面上查找登录输入框，以及登录按钮，登录成功后，还会在页面上识别退出登录的触发链接，避免登出。查找这些元素的成功率受影响于用户站点页面元素的复杂程度。

如果扫描任务自动登录失败，可能是因为您的网站需要登录才能访问，请检查您是否通过漏洞扫描服务对您的网站进行了正确的网站登录信息配置，请参照以下操作步骤设置网站登录方式或者修改网站登录配置信息。

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击 ☰，选择“安全 > 漏洞扫描服务”，进入漏洞扫描服务页面。

步骤 3 在“资产列表 > 网站”页签，进入网站列表入口。

步骤 4 在目标域名的“操作”列，单击“编辑”，进入域名编辑页面，根据需要修改“网站登录设置”，如图 10-4 所示。

图10-4 编辑页面

步骤 5 单击“确认”。

----结束

10.2.4 创建网站扫描任务或重启任务不成功时如何处理？

请执行以下步骤进行处理。

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击 ☰，选择“安全 > 漏洞扫描服务”，进入漏洞扫描服务页面。

步骤 3 在“资产列表 > 网站”页签，进入网站列表入口。

步骤 4 在“资产列表”界面，查看目标网址是否已完成域名认证。

- 如果是，请联系技术支持。
- 如果否，请执行步骤 5～步骤 6 完成域名认证。

步骤 5 在目标域名的“认证状态”列，单击“前往认证”。

步骤 6 在弹出的“认证域名”对话框中，选择域名认证方式完成域名认证。

- 一键认证，如图 10-5 所示。

图10-5 一键认证方式

----结束

10.2.5 网站漏洞扫描一次需要多久？

网站漏洞扫描的时长，跟多种因素相关，包括网站规模（即自动爬取的页面数）、网站响应速度、页面复杂度、网络环境等，通常扫描时长为小时级别，最长不超过 24 小时。

测试环境下，200 个页面的网站完成一次全量扫描耗时约 1 个小时，这里仅供参考，请以实际扫描时间为准。

另外扫描的过程中会向网站发送一定数量的检测请求，可能会导致网站的负载小幅度增大。

10.2.6 为什么任务扫描中途就自动取消了？

如果一个任务扫描到一半被系统自动取消了，可能有以下两个原因：

- 没有配置“网站登录设置”信息。

  用户没有配置“网站登录设置”信息，VSS 无法进行深入的访问，任务就会自动取消。 建议设置“网站登录设置”信息后，重新扫描。
- 扫描过程中，出现了网络问题。

  网络异常，VSS 将无法访问网站，任务就会自动取消。建议网络正常后，重新扫描。

10.2.7 如何设置定时扫描？

在创建任务时，设置“开始时间”，设置好启动时间后，系统会在用户设置的时间点启动该任务，如图 10-6 所示。

说明

启动时间必须在一周之内。

图10-6 定时开始

10.2.8 创建任务时为什么总是提示域名格式错误？

创建任务时，为了让漏洞扫描服务识别出网站使用的协议（http 或 https），需要在输入的时候填写此信息。

正确的域名格式为：“http(s)://域名或 IP”。

例如：一个使用 https 协议，IP 地址为 10.10.10.1 的网站，在创建任务时应输入的“目标网址”为“https://10.10.10.1”。

10.2.9 如何对网站进行域名认证？

执行以下步骤进行域名认证：

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击 ☰，选择“安全 > 漏洞扫描服务”，进入漏洞扫描服务页面。

步骤 3 在“资产列表 > 网站”页签，单击“去认证”。

步骤 4 进入域名认证入口，如图 10-7 所示。

图10-7 进入域名认证页面

步骤 5 在弹出的“认证域名”对话框中，选择域名认证方式完成域名认证。

- 免认证，仔细阅读图 10-8 中的使用须知，确认符合条件后，完成域名认证。

图10-8 免认证方式

- 一键认证，如图 10-9 所示。

图10-9 一键认证方式

----结束

10.2.10 如何解决网站扫描失败，报连接超时的问题？

网站扫描任务失败，报错为连接超时，可能原因与解决办法如下。

1. 您的被测网站不稳定或无法通过互联网访问，请使用 Chrome 等浏览器访问网站，确认是否正常访问。
2. 您的网站设置了防火墙或其他安全策略，导致漏洞扫描的引擎 IP 被当成恶意攻击而拦截。请参见漏洞扫描服务的扫描 IP 有哪些？为漏洞扫描引擎设置访问白名单。

10.2.11 漏洞扫描服务支持 web_CMS 漏洞吗？

VSS 暂不支持 web_CMS 漏洞扫描功能。

10.2.12 标准策略、极速策略和深度策略有哪些区别？

VSS 提供支持以下 3 种网站扫描模式：

- “极速策略”：扫描的网站 URL 数量有限且 VSS 会开启耗时较短的扫描插件进行扫描。
- “深度策略”：扫描的网站 URL 数量不限且 VSS 会开启所有的扫描插件进行耗时较长的遍历扫描。
- “标准策略”：扫描的网站 URL 数量和耗时都介于“极速策略”和“深度策略”两者之间。

有些接口只能在登录后才能访问，建议用户配置对应接口的用户名和密码，VSS 才能进行深度扫描。

10.2.13 已添加的域名是否可以删除？

可以删除，但域名删除后，该资产的历史扫描数据将被删除，不可恢复。

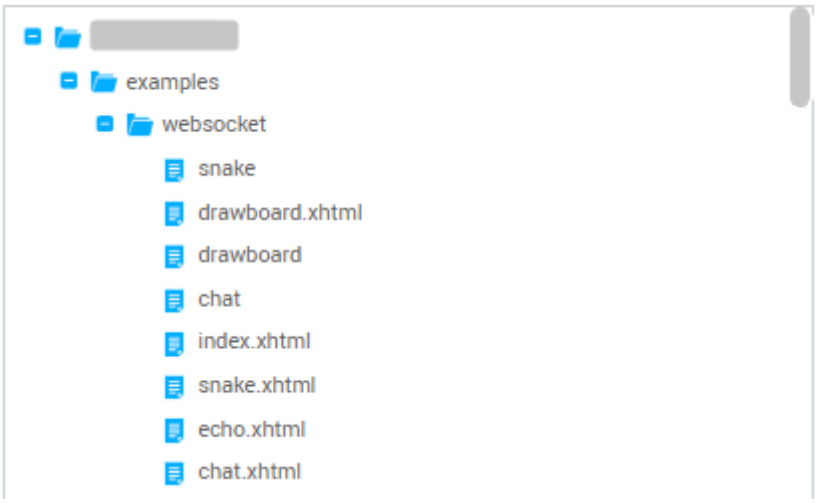
10.2.14 如何查看漏洞扫描服务扫描出的网站结构？

执行完漏洞扫描任务后，进入“总览”页面，在“最近扫描任务列表”中，单击目标扫描对象，进入任务详情页面，单击“站点结构”页签，查看网站结构。

说明

站点结构展示的是任务扫描出的漏洞对应的网页地址及整体结构，如果任务暂未扫描出漏洞，站点结构无数据显示。

图10-10 查看站点结构



10.2.15 如何获取网站 cookie 值？

如果您的网站除了需要账号密码登录，还有其他的访问机制（例如，需要输入动态验证码），则建议您设置 cookie 登录方式进行网站漏洞扫描，以便 VSS 能为您发现更多安全问题。

设置 cookie 登录方式时需要输入网站的 cookie 值。

须知

获取 cookie 值后，在创建扫描任务时，请您保持网站的登录状态，以免 cookie 失效。

以 Google Chrome 浏览器为例说明，获取网站（例如，www.example.com）的 cookie 值的步骤如下：

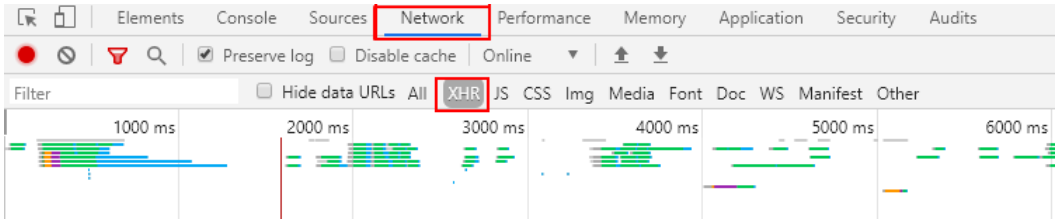
步骤 1 打开 Google Chrome 浏览器。

步骤 2 按“F12”，进入浏览器的开发者模式。

步骤 3 在地址栏中输入目标网站地址“www.example.com”。

步骤 4 在调试页面中，选择“Network > XHR” ，如图 10-11 所示。

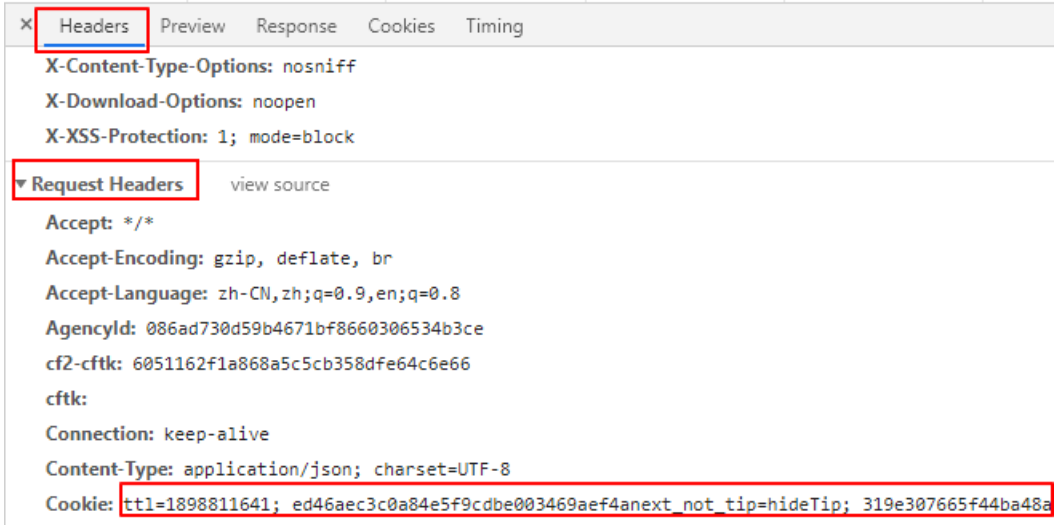
图10-11 Network 页面



步骤 5 在左侧导航树中，选择一个 http 请求。

步骤 6 在“Headers”页面的“Request Headers”区域框，获取当前网站页面的“Cookie”字段值，如图 10-12 所示。

图10-12 获取 cookie 值



----结束

10.2.16 网站 cookie 值发生变化时，如何进行网站漏洞扫描？

当某个网站挂载多个子网站，且需要对这些网站都进行漏洞扫描（使用 cookie 登录方式）时，如果您从网站主入口登录后，再进入其他子网站，网站的 cookie 值可能会发生改变。对于 cookie 值发生改变的子网站，您需要为这些子网站单独完成扫描任务的创建。

10.2.17 如何处理域名认证时提示“域名已被其他人使用”？

对域名进行认证时，如果提示域名已被其他人使用，说明该域名已被其他帐号进行认证。一般情况下，能够认证该域名的帐号应隶属于您的单位，请咨询您的同事是否用了其他帐号认证了该域名，或者您也可以提工单咨询域名认证情况。

10.2.18 漏洞扫描服务可以扫描域名下的项目吗？

VSS 采用网页爬虫的方式全面深入的爬取网站 url，然后针对爬取出来的页面模拟黑客进行试探攻击，帮助您发现网站潜在的安全隐患。如果域名下的项目没有被 VSS 爬取出来，则该项目不会被 VSS 扫描到。您可以通过网站扫描详情，查看域名下的项目是否被 VSS 扫描到。

10.3 主机扫描类

10.3.1 VSS 的主机扫描 IP 有哪些？

如果设置了访问限制，请添加策略允许 VSS 的 IP 地址可以访问您的主机。如果您使用了主机安全防护软件，请将 VSS 访问主机的 IP 地址添加到该软件的白名单中，以免该软件拦截了 VSS 访问用户主机的 IP 地址。

114.217.39.79，222.93.127.109

10.3.2 为什么主机添加成功后不能在主机列表中查找到？

由于 VSS 系统处理任务需要一段时间，因此主机添加成功后您不能在主机列表中马上查找到该添加的主机。请您等待一段时间，刷新主机列表再查找添加的主机。

10.3.3 如何对主机进行授权？

操作场景

该任务指导用户通过漏洞扫描服务对已添加的 Linux 主机进行扫描授权。

前提条件

- 已获取管理控制台的登录账号与密码。
- 已添加 Linux 主机。

操作步骤

步骤 1 登录管理控制台。

步骤 2 选择“安全 > 漏洞扫描服务”，进入漏洞扫描服务管理控制台。

步骤 3 在左侧导航栏，选择“资产列表 > 主机”，进入主机列表入口。

步骤 4 批量选择需要配置的主机，单击“批量操作 > 编辑”，进入批量授权入口，如图 10-13 所示。

图10-13 进入批量授权入口

说明

用户也可以单台主机授权，在目标主机所在行的“操作”列，单击“编辑”。

步骤 5 在主机授权页面，批量选择需要授权的主机，单击“批量配置授权信息”，如图 10-14 所示。

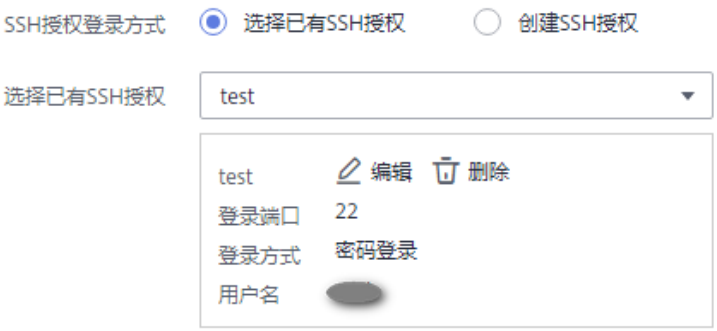
说明

- 用户也可以单台主机授权，在目标主机所在行的“操作”列，单击“配置授权信息”。
- 如果需要修改主机名称，单击，在弹出的对话框中，进行修改。

图10-14 批量授权

步骤 6 选择 SSH 授权方式进行主机授权。

图10-15 SSH 授权登录



说明

- 如果需要修改已有 SSH 授权，单击“编辑”，进行修改。
- 如果需要删除已有 SSH 授权，单击“删除”，进行删除。

选择已有 SSH 授权，或者单击“创建 SSH 授权”创建 SSH 授权，如图 10-16 所示，参数说明如表 10-4 所示。

图10-16 创建 SSH 授权

表10-4 参数说明

参数名称	参数说明
SSH 授权别称	自定义 SSH 授权名称。
登录端口	SSH 授权登录的端口号。 请确保安全组已添加该端口，以便主机可通过该端口访问 VSS。
选择登录方式	• “密码登录” • “密钥登录”
选择加密密钥	为了保护主机登录密码或密钥安全，请您必须使用加密密钥，以避免登录密码或密钥明文存储和泄露风险。 您可以选择已有的加密密钥，如果没有可选的加密

参数名称	参数说明
	密钥，请单击“创建密钥”，创建 VSS 专用的默认主密钥。
Root 权限是否加固	打开该权限后，不可以用 root 账号直接登录，而只能通过普通用户登录，然后才能切换到 root 用户。
sudo 用户名	默认为 root。
sudo 密码	设置 sudo 用户对应的密码，为了您的账号安全，您的密码会加密保存。

步骤 7 单击“确认”，完成 Linux 主机授权。

步骤 8 单击“确定”，Linux 主机授权成功。

----结束

10.3.4 漏洞扫描服务支持哪些操作系统的主机扫描？

漏洞扫描服务支持扫描的主机操作系统版本如下：

支持的 Linux 操作系统版本，如表 10-5 所示。

支持的 Windows 操作系统版本，如表 10-6 所示。

表10-5 Linux 操作系统版本

分类	支持的 OS 类型
EulerOS	EulerOS 2.2, 2.3, 2.5, 2.8 and 2.9 64bit
CentOS	CentOS 6.5, 6.8, 6.9, 6.10, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8 and 7.9 64 bit
RedHat	Red Hat Enterprise Linux 6.10 and 7.5 64bit
Ubuntu	Ubuntu 16.04, 18.04 and 20.04 server 64bit
SUSE	SUSE Enterprise 11 SP4 64bit, SUSE Enterprise 12 SP1/SP2/SP3/SP4 64bit, SUSE Enterprise 15 SP1/SP2 64bit
OpenSUSE	OpenSUSE 13.2 and 42.2 64bit
Debian	Debian 8.2.0, 8.8.0, 9.0.0, 10.0.0 64bit
Kylin OS	Kylin OS V10 SP1 64bit
统信 UOS	V20
Huawei Cloud EulerOS	HCE 2.0

表10-6 Windows 操作系统版本

分类	支持的 Windows 系统版本
Windows Server	Windows Server 2012 R2，Windows Server 2016

10.3.5 如何修复扫描出来的主机漏洞？

不同的主机系统修复漏洞的方法有所不同，软件漏洞的修复需要具有一定专业知识的人员进行操作，根据服务器的情况进行漏洞修复，可参考漏洞扫描服务给出的修复建议，修复漏洞时应按照如下的操作步骤进行修复。

步骤 1 对需要修复的服务器实例进行备份，防止出现不可预料的后果。

步骤 2 对需要修复的资产和漏洞进行多次确认。根据业务情况以及服务器的使用情况等综合因素，确认自己的资产是否需要做漏洞修复，并形成漏洞修复列表。

步骤 3 在模拟测试环境中部署待修复漏洞的相关补丁，从兼容性和安全性方面进行测试，并输出补丁漏洞修复测试报告，报告内容应包含补丁漏洞修复情况、漏洞修复的时长、补丁本身的兼容性、以及漏洞修复可能造成的影响。

步骤 4 进行漏洞修复时，最好多人在场，边操作边记录，防止出现误操作。

步骤 5 漏洞修复完成后，在测试环境对目标服务器系统上的漏洞进行修复验证，确保服务器没有异常，输出详细的修复记录进行归档，方便日后遇见相关问题可快速反应。

----结束

总之，为了防止在漏洞修复过程中出现问题，在漏洞修复前要及时备份、制定方案、在测试环境进行模拟测试验证可行性，在修复过程中要小心并及时记录，在修复后及时生成完备的修复报告进行归档。

10.3.6 漏洞扫描服务可以扫描本地的物理服务器吗？

漏洞扫描服务可以扫描本地的物理服务器。若需要扫描本地的物理服务器，需要满足以下条件。

- 本地网络可通外网。
- 本地物理服务器为 Linux 操作系统，且满足以下版本要求：
  - EulerOS：支持的最低系统版本为 EulerOS 2.2。
  - CentOS：支持的最低系统版本为 CentOS 6.5。
  - RedHat：支持的最低系统版本为 Red Hat Enterprise Linux 6.10。
  - Ubuntu：支持的最低系统版本为 Ubuntu 16.04 server。
  - SUSE：支持的最低系统版本为 SUSE Enterprise 11 SP4。
  - OpenSUSE：支持的最低系统版本为 OpenSUSE 13.2。
  - Debian：支持的最低系统版本为 Debian 8.2.0。
  - Kylin OS：支持的系统版本为 Kylin OS V10 SP1。
- 可以远程登录到本地物理服务器。

本地物理服务器满足以上条件后，可以在漏洞扫描服务界面通过添加跳板机的方式，使用漏洞扫描服务扫描本地的物理服务器。

有关物理服务器使用 VSS 的详细介绍，请参见物理服务器可以使用漏洞扫描服务吗？。

10.3.7 物理服务器可以使用漏洞扫描服务吗？

当您的物理服务器为 Linux 操作系统，且满足以下版本要求时，如果您的物理服务器可以远程登录，则可以通过添加跳板机的方式使用漏洞扫描服务。

- EulerOS：支持的最低系统版本为 EulerOS 2.2。
- CentOS：支持的最低系统版本为 CentOS 6.5。
- RedHat：支持的最低系统版本为 Red Hat Enterprise Linux 6.10。
- Ubuntu：支持的最低系统版本为 Ubuntu 16.04 server。
- SUSE：支持的最低系统版本为 SUSE Enterprise 11 SP4。
- OpenSUSE：支持的最低系统版本为 OpenSUSE 13.2。
- Debian：支持的最低系统版本为 Debian 8.2.0。
- Kylin OS：支持的系统版本为 Kylin OS V10 SP1。

操作步骤

步骤 1 登录管理控制台。

步骤 2 选择“安全 > 漏洞扫描服务”，进入漏洞扫描服务管理控制台。

步骤 3 在左侧导航栏，选择“资产列表 > 主机”，进入主机列表入口。

步骤 4 在“添加主机”页面，单击“添加主机”，参数说明如表 10-7 所示。

图10-17 添加主机

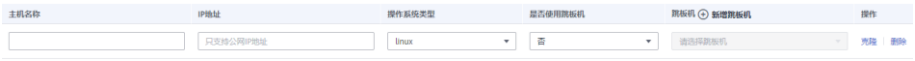


表10-7 参数说明

参数名称	参数说明	配置示例
主机名称	用户需要添加的主机名称。	vss-test
IP 地址	添加主机的公网 IP 地址。	192.168.2.3
是否使用跳板机	选择“是”。	是
跳板机	可在下拉框中选择已有跳板机，或者单击“新增跳板机”，添加跳板机。	-

步骤 5 新增跳板机。

1. 单击“新增跳板机”。
2. 在弹出的对话框中，设置跳板机参数，如图 10-18 所示，相关参数说明如表 10-8 所示。

图10-18 添加跳板机

表10-8 跳板机配置参数说明

参数名称	参数说明
主机名称	添加的跳板机的主机名称。
公网 IP	添加的跳板机的公网 IP。
登录端口	添加的跳板机的登录端口。
选择登录方式	“密码登录”和“密钥登录”。 • 选择密码登录时，需要添加跳板机的用户名和密码。 • 选择密钥登录时，需要添加跳板机的用户名、私钥和私钥密码。
选择加密密钥	为了保护主机登录密码或密钥安全，请您必须使用加密密钥，以避免登录密码或密钥明文存储和泄露风险。 您可以选择已有的加密密钥，如果没有可选的加密密钥，请单击“创建密钥”，创建 VSS 专用的默认主密钥。

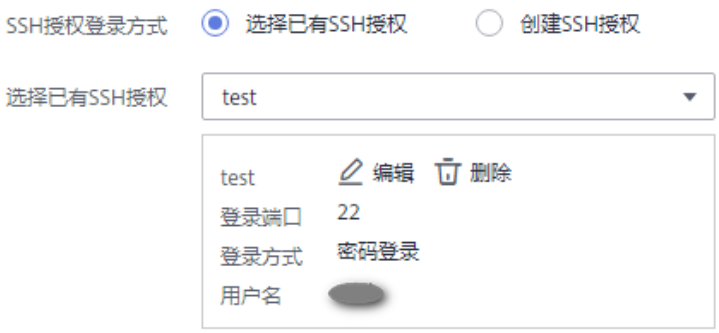
3. 单击“确认”。

步骤 6 单击“下一步”，添加主机完成。

步骤 7 在添加的主机所在行的“操作”列，单击“配置授权信息”。

步骤 8 选择 SSH 授权方式进行主机授权。

图10-19 SSH 授权登录



说明

- 如果需要修改已有 SSH 授权，单击“编辑”，进行修改。
- 如果需要删除已有 SSH 授权，单击“删除”，进行删除。

选择已有 SSH 授权，或者单击“创建 SSH 授权”创建 SSH 授权，如图 10-20 所示，参数说明如表 10-9 所示。

图10-20 创建 SSH 授权

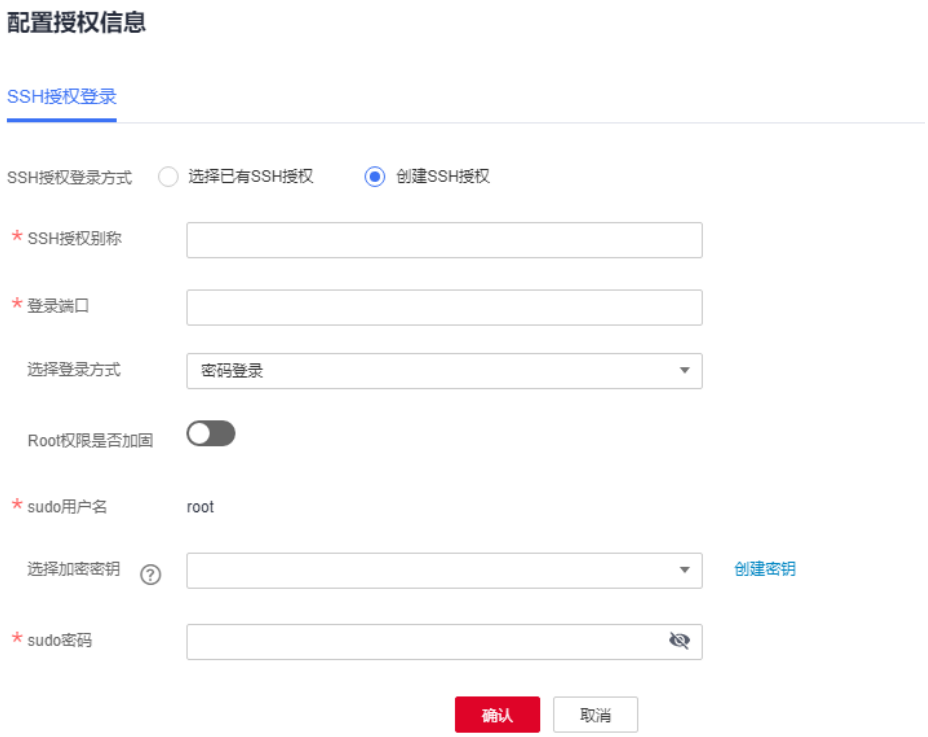


表10-9 参数说明

参数名称	参数说明
SSH 授权别称	自定义 SSH 授权名称。
登录端口	SSH 授权登录的端口号。 请确保安全组已添加该端口，以便主机可通过该端口访问 VSS。
选择登录方式	• “密码登录” • “密钥登录”
选择加密密钥	为了保护主机登录密码或密钥安全，请您必须使用加密密钥，以避免登录密码或密钥明文存储和泄露风险。 您可以选择已有的加密密钥，如果没有可选的加密密钥，请单击“创建密钥”，创建 VSS 专用的默认主密钥。
Root 权限是否加固	打开该权限后，不可以用 root 账号直接登录，而只能通过普通用户登录，然后才能切换到 root 用户。
sudo 用户名	默认为 root。

参数名称	参数说明
sudo 密码	设置 sudo 用户对应的密码，为了您的账号安全，您的密码会加密保存。

步骤 9 单击“确定”，完成主机授权。

----结束

10.3.8 如何创建 SSH 授权？

Linux 主机支持“SSH 授权登录”授权方式。

添加 Linux 主机后，请参照以下操作步骤创建 SSH 授权。

步骤 1 登录管理控制台。

步骤 2 选择“安全 > 漏洞扫描服务”，进入漏洞扫描服务管理控制台。

步骤 3 在左侧导航栏，选择“资产列表 > 主机”，进入主机列表入口。

步骤 4 批量选择需要配置的主机，单击“批量操作 > 编辑”，进入批量授权入口，如图 10-21 所示。

图10-21 进入批量授权入口

说明

用户也可以单台主机授权，在目标主机所在行的“操作”列，单击“编辑”。

步骤 5 在主机授权页面，批量选择需要授权的主机，单击“批量配置授权信息”，如图 10-22 所示。

说明

- 用户也可以单台主机授权，在目标主机所在行的“操作”列，单击“配置授权信息”。
- 如果需要修改主机名称，单击，在弹出的对话框中，进行修改。

图10-22 批量授权

步骤 6 选择已有 SSH 授权，或者单击“创建 SSH 授权”创建 SSH 授权，如图 10-23 所示，参数说明如表 10-10 所示。

图10-23 创建 SSH 授权

表10-10 参数说明

参数名称	参数说明
SSH 授权别称	自定义 SSH 授权名称。
登录端口	SSH 授权登录的端口号。 请确保安全组已添加该端口，以便主机可通过该端口访问 VSS。

参数名称	参数说明
选择登录方式	• “密码登录” • “密钥登录”
选择加密密钥	为了保护主机登录密码或密钥安全，请您必须使用加密密钥，以避免登录密码或密钥明文存储和泄露风险。 您可以选择已有的加密密钥，如果没有可选的加密密钥，请单击“创建密钥”，创建 VSS 专用的默认主密钥。
Root 权限是否加固	打开该权限后，不可以用 root 账号直接登录，而只能通过普通用户登录，然后才能切换到 root 用户。
sudo 用户名	默认为 root。
sudo 密码	设置 sudo 用户对应的密码，为了您的账号安全，您的密码会加密保存。

步骤 7 单击“确认”，完成 Linux 主机授权。

----结束

10.3.9 配置主机授权时，必须使用加密密钥吗？

在创建 SSH 授权登录（Linux 主机）时，为了保护主机登录密码或密钥安全，请您必须使用加密密钥，以避免登录密码或密钥明文存储和泄露风险。

您可以选择已有的加密密钥，如果没有可选的加密密钥，请单击“创建密钥”，创建 VSS 专用的默认主密钥。

有关配置主机授权的详细操作，请参见如何对主机进行授权？。

10.3.10 创建 SSH 授权时，如何设置登录端口？

在为 Linux 主机创建 SSH 授权登录时，需要设置登录端口，如图 10-24 所示。

在设置登录端口时，请确保安全组已添加该端口，以便主机可通过该端口访问 VSS。

图10-24 设置登录端口

10.3.11 如何扫描修改了 IP 地址的主机？

如果您的主机已在本地配置了账号和密码，当您修改该主机的 IP 地址后，请先在本地重新配置该主机的账号和密码，然后在漏洞扫描服务中添加该主机并授权漏洞扫描服务可以访问该主机。

有关对主机进行授权的详细操作，请参见如何对主机进行授权？。

10.3.12 对主机扫描出的漏洞执行“忽略”操作有什么影响？

在扫描详情页面中，如果您确认扫描出的漏洞不会对主机造成危害，您可以在目标漏洞所在行的“操作”列，单击“忽略”，忽略该漏洞，后续执行扫描任务会扫描出该漏洞，但相应的漏洞统计结果将发生变化，扫描报告中也不会出现该漏洞。

10.3.13 主机扫描可以关闭基线检查吗？

主机扫描不能关闭基线检查。如果您确认基线检查扫描出的检查项不会对主机造成危害，您可以在目标检查项所在行的“操作”列，单击“忽略”，忽略该检查项，相应的检查项统计结果将发生变化，扫描报告中也不会出现该检查项。

10.3.14 基线检查的风险个数是如何统计的？

基线检查结果中“未通过”的检查项的总数即为基线检查的风险个数。

10.3.15 等保合规的检查项可以忽略吗？

可以。

- 如果您确认扫描出的检查项不会对主机造成危害，您可以在目标检查项所在行的“操作”列，单击“忽略”，忽略该检查项，后续执行扫描任务会扫描出该漏洞，但相应的检查项统计结果将发生变化，扫描报告中也不会出现该检查项。
- VSS 目前仅企业版用户支持等保合规检测，如果您需要对您的主机进行等保合规检测，请购买企业版。

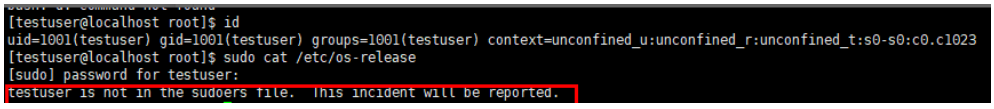
10.3.16 基线检查总数与检查项数不一致，为什么？

VSS 目前仅支持扫描一个 tomcat 进程，当目标主机有多个 tomcat 进程时，基线检查的总扫描数与检查项显示的个数不一致。

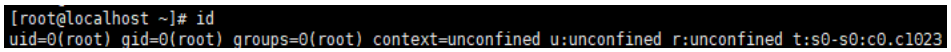
请您保留一个 tomcat 进程后，重新对该目标主机进行扫描。

10.3.17 配置普通用户和 sudo 提权用户漏洞扫描失败案例

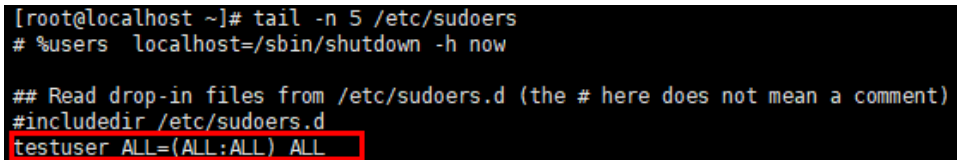
默认情况下，Linux 系统没有将普通用户列入到 sudoer 列表中（普通用户 is not in the sudoers file. This incident will be reported.）：



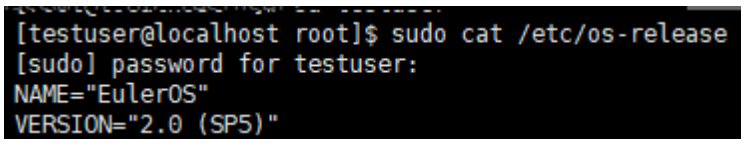
1. 登录系统并切换到 root 权限。

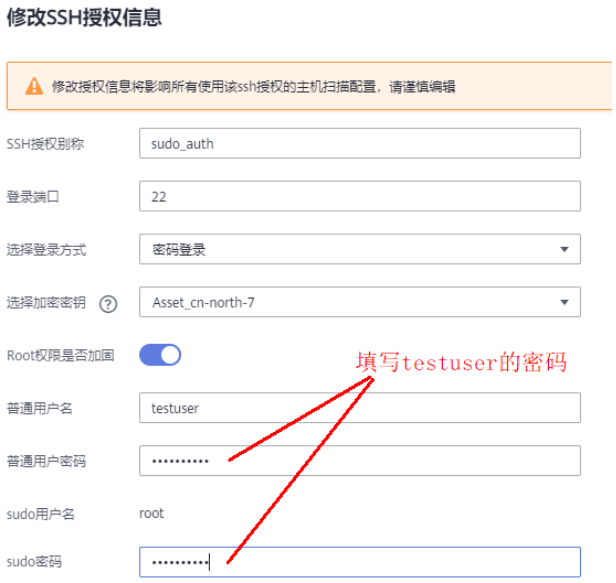
2. 输入#vi /etc/sudoers，就会打开 sudoers 配置文件。
3. 在配置文件末尾添加：普通用户名 ALL=(ALL:ALL) ALL，输入 :wq! ，保存修改。

说明



- 使用 VSS 的 sudo 提权扫描功能时，认证凭据输入位置的“普通用户密码”和“sudo 密码”请保持一致，均为“普通用户”的密码。

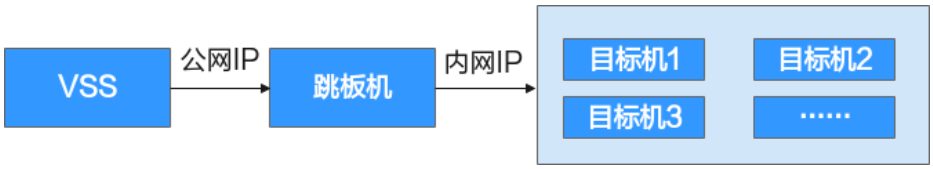


- 扫描完成后，请还原配置。

10.3.18 如何配置跳板机进行内网扫描？

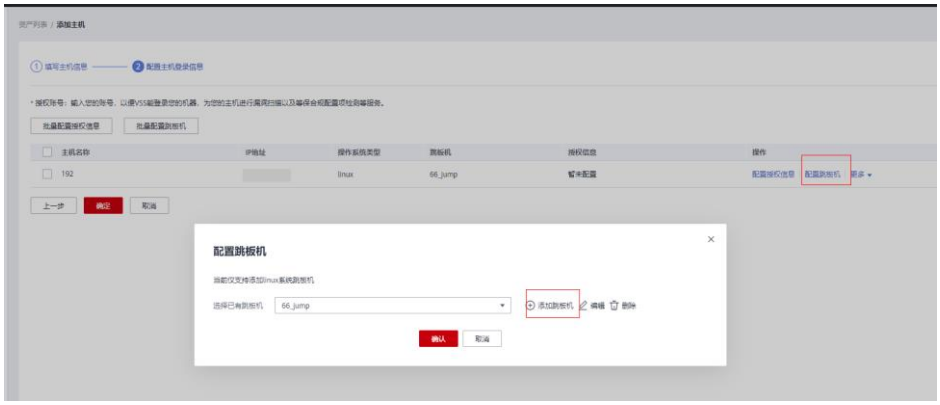
使用跳板机进行内网扫描的网络示意图如图 10-25 所示。

图10-25 网络示意图



1. 创建主机扫描任务，IP 地址栏填写目标主机的内网 IP。
2. 添加跳板机配置。

   配置的跳板机“公网 IP”需与被测目标机的内网环境互通。



添加跳板机后，还需在该跳板机的 ssh 配置文件“/etc/ssh/sshd_config”中添加：AllowTcpForwarding yes，用于支持 SSH 授权登录转发。修改配置后需重启 sshd 服务。

10.3.19 为什么安装了最新 kernel 后，仍报出系统存在低版本 kernel 漏洞未修复？

使用 yum update kernel 将 kernel 更新至最新版本后，VSS 扫描 EulerOS 仍报出大量 kernel 漏洞。这种情况不属于 VSS 工具误报，而是由于升级 kernel 之后未及时重启并使用最新版本的 kernel 运行。kernel 升级到最新版本后未重启并运行，实际上仍然使用未升级前的 kernel 扫描系统，所以漏洞仍然存在。

- 执行 如下命令可以查看当前系统安装了哪些版本的 kernel。

```
rpm -qa | grep kernel
```

```
[root@localhost ~]# rpm -qa |grep kernel
kernel-tools-4.18.0-147.5.1.2.h340.eulerosv2r9.x86_64
kernel-tools-libs-4.18.0-147.5.1.2.h340.eulerosv2r9.x86_64
kernel-4.18.0-147.5.1.6.h579.eulerosv2r9.x86_64
kernel-4.18.0-147.5.1.2.h340.eulerosv2r9.x86_64
kernel-headers-4.18.0-147.5.1.6.h579.eulerosv2r9.x86_64
```

- 执行如下命令可以查看当前系统实际使用的是什么版本的 kernel。

```
uname -a
```

```
[root@localhost ~]# uname -a
Linux localhost.localdomain 4.18.0-147.5.1.2.h340.eulerosv2r9.x86_64 #1
```

⚠ 注意

- 上面例子中就是实际使用的是低版本的存在大量 CVE 漏洞的 kernel，因此使用 VSS 扫描仍会报 kernel 存在 CVE-2020-0465 等漏洞。
- 此案例对于使用了 CentOS、EulerOS、Red Hat、SUSE 的用户均适用。
- 此外还有某些情况下，用户使用的 yum 源并不是操作系统官方最新的源，也即 yum 源中没有操作系统最新的安全补丁，此种情况下也可能报出 kernel 漏洞未修复的问题。此种情况下需要更新 yum 源为操作系统官方源或者向操作系统提供方寻求安全补丁的支持。总之，需要基于 VSS 扫描报告中的“修复建议”中的 installed version 和 fixed version 的内容，进行分析和修复。

10.3.20 使用跳板机扫描内网主机和直接扫描公网主机，在扫描能力方面有什么区别？

使用跳板机扫描内网主机和直接扫描公网主机，在扫描能力方面区别如表 10-11 所示。

表10-11 扫描能力差异介绍

扫描能力	通过公网 IP 直接扫描公网主机	通过跳板机扫描内网主机
操作系统安全补丁扫描	支持	支持

扫描能力	通过公网 IP 直接扫描公网主机	通过跳板机扫描内网主机
远程服务/协议漏洞扫描	支持	不支持 说明 远程服务/协议类漏洞的扫描依赖于扫描器与被测目标的相关端口直接交互，因此不能通过跳板机完成测试验证。
操作系统安全配置扫描	支持	支持
Web 中间件安全配置扫描	支持	支持
等保合规扫描	支持	支持

10.4 计费类

10.4.1 漏洞扫描服务如何收费？

计费项

VSS 根据您的 VSS 服务版本，扫描配额包的个数和购买时长计费。

表10-12 计费项信息

计费项目	计费说明
服务版本（必选）	按购买的服务版本（基础版、专业版、高级版或企业版）计费。
扫描配额包	按购买的个数计费。
购买时长	提供包年/包月和按需计费的购买模式。

计费模式

VSS 提供按需计费和包年/包月两种计费模式，用户可以根据实际需求选择计费模式。

表10-13 VSS 各服务版本计费方式

服务版本	支持的计费方式	说明

服务版本	支持的计费方式	说明
基础版	• 配额内的服务免费 • 按需计费	• 基础版配额内仅支持 Web 网站漏洞扫描（域名个数：5 个，扫描次数：每日 5 次）是免费的。 • 基础版提供的以下功能按需计费： 1. 可以将 Web 漏洞扫描或主机漏洞扫描任务升级为专业版规格进行扫描，扫描完成后进行一次性扣费。 2. 主机扫描一次最多支持 20 台主机。
专业版	包年/包月	相对于按需付费，包年/包月购买方式能够提供更大的折扣，对于长期使用者，推荐该方式。包周期计费为按照订单的购买周期来进行结算。不限制扫描次数。
高级版		
企业版		

变更配置

- 域名配额扩容：当您的业务需求增加，可在计费周期内“扩容”域名的扫描配额包。支持扩容**专业版配额**、**高级版配额**以及**企业版配额**。不支持多个版本同时存在。
- 专业版升级为高级版：当您是专业版用户时，如果需要将专业版扫描配额包中的二级域名配额全部升级为一级域名配额，可以直接将**专业版**升级为**高级版**。
- 退订：购买漏洞扫描服务的扫描配额包后，如需停止使用，

续费

扫描配额包到期后，您可以进行续费以延长扫描配额包的有效期，也可以设置到期自动续费。

到期与欠费

包周期资源开通成功后，如果没有按时续费，平台会提供一定的保留期。

欠费后，可以查看欠费详情。为防止相关资源不被停止或者释放，请及时进行充值，帐号将进入欠费状态，需要在约定时间内支付欠款。

10.4.2 退订重购 VSS 后，是否需要重新配置域名信息？

不需要。

版本的变化（购买、变更、退订等）不会修改或删除已配置的域名信息，因此，不需要重新配置。

10.4.3 购买专业版漏洞扫描服务的注意事项？

如果您在购买专业版之前使用过免费体验版（即基础版）进行扫描，在购买专业版时，“扫描配额包”的选择必须等于或者大于当前资产列表已添加的网站个数。

- 如果当前资产列表的某个基础版域名，您不想升级为专业版为其付费，请您在购买专业版之前对其进行删除。
- 如果您只需要将当前基础版域名全部升级为专业版规格，“扫描配额包”的选择等于当前资产列表已添加的网站个数。
- 如果您需要增加域名配额，即增加扫描的网站个数，“扫描配额包”的选择大于当前资产列表已添加的网站个数，且“扫描配额包”的选择值为您期望的域名配额值。

购买成功后，当前资产列表所有基础版域名默认升级为专业版，享受专业版规格。

10.5 报告类

10.5.1 如何下载网站扫描报告？

操作场景

当网站扫描任务成功完成后，您可以下载任务报告，报告目前只支持 PDF 格式。

前提条件

已成功完成网站扫描任务，即目标域名的“上一次扫描结果”状态为“已完成”。

操作步骤

步骤 1 登录管理控制台。

步骤 2 在左侧导航树中，单击 ☰，选择“安全 > 漏洞扫描服务”，进入漏洞扫描服务页面。

步骤 3 在“资产列表 > 网站”页签，进入下载网站扫描报告入口，如图 10-26 所示。

图10-26 进入下载网站扫描报告入口

步骤 4 单击右上角的 生成报告，生成网站扫描报告，如图 10-27 所示。

如果报告已生成，则可跳过此步。

图10-27 生成扫描报告

说明

生成的扫描报告会在 24 小时后过期。过期后，若需要下载扫描报告，请再次单击“生成报告”，重新生成扫描报告。

步骤 5 扫描报告生成完成后，单击右上角的 下载报告，将网站扫描报告下载到本地，如图 10-28 所示。

图10-28 下载扫描报告

----结束

10.5.2 漏洞扫描报告模板包括哪些内容？

当扫描任务成功完成后，您可以下载任务报告，报告目前只支持 PDF 格式。

网站漏洞扫描报告模板说明

下载扫描报告后，您可以根据扫描结果，对漏洞进行修复，报告模板主要内容说明如下：

- 概览

  查看目标网站的扫描漏洞数。

图10-29 查看任务概览信息

1 概览

1.1 任务综述

本次扫描检测出漏洞总数 29 个，漏洞类型 4 种。其中高危漏洞有 1 个。

任务名称	ecshop3
扫描对象	http://
开始时间	2020-09-22 11:04:50
结束时间	2020-09-22 11:13:01
扫描耗时	1.34小时

1.2 网站指纹信息

IP	
服务器	OPENRESTY[ ];NGINX
编程语言	PHP[5.6.37];LUA
开放端口	8080, 8081

- 漏洞分析概览

  统计漏洞类型及分布情况。

图10-30 漏洞类型分析

2 漏洞分析概览

2.1 扫描概览

扫描分数&漏洞个数					
4 分	总漏洞数	高危漏洞	中危漏洞	低危漏洞	提示威胁
	29	1	1	27	0

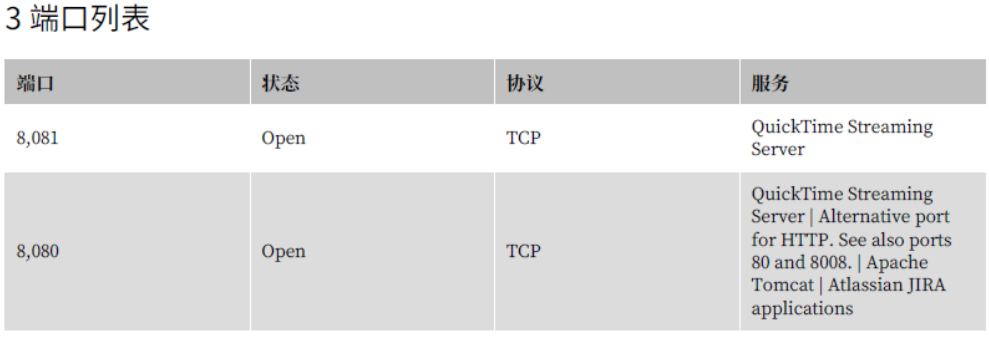
2.2 漏洞类型分布

分类	漏洞类型	检测结果
恶意内容	恶意外链	安全
	挖矿后门	安全
	网页木马	安全
潜在风险	网站请求头	4个风险项
	Https协议	安全
网站安全漏洞	跨站请求伪造	安全
	应急漏洞	安全
	信息泄露	16个漏洞 查看详情
	注入攻击	安全
	其它	4个漏洞 查看详情
	路径遍历	安全
	授权问题	安全
	弱密码	1个漏洞 查看详情
	跨站脚本攻击	8个漏洞 查看详情

- 服务端口列表

  查看目标网站的所有端口信息。

图10-31 网站的端口列表



3 端口列表

端口	状态	协议	服务
8,081	Open	TCP	QuickTime Streaming Server
8,080	Open	TCP	QuickTime Streaming Server | Alternative port for HTTP. See also ports 80 and 8008. | Apache Tomcat | Atlassian JIRA applications

- 漏洞根因及详情

  您可以根据修复建议修复漏洞。

图10-32 漏洞根因及详情

5.2 应急漏洞

序号	漏洞名称	漏洞级别	漏洞个数
1	Fastjson远程代码执行漏洞	高危	1

5.2.1 Fastjson远程代码执行漏洞

漏洞级别 高危

漏洞简介

[redacted]关注到Fastjson 存在反序列化远程代码执行漏洞，可导致直接获取服务器权限，且此漏洞为 17 年 Fastjson 1.2.24 版本反序列化漏洞的延伸利用，危害严重。此漏洞影响版本 < 1.2.51，请受影响的用户尽快升级至安全版本。

修复建议

1)方案一：升级 fastjson，升级到最新版本1.2.58，下载地址：https://github.com/[redacted]/fastjson/releases/tag/1.2.58;
2)方案二：移除 fastjson，如需使用 json 解析库建议使用 gson 或 jackson-databind 等组件最新版本替换。

问题URL列表

序号	影响URL	发现时间
1	http://[redacted]	2019-07-12 22:11:29

5.2.1.1 http://[redacted]

发现时间 2019-07-12 22:11:29

命中详情 "{[redacted]}"

请求详情

[redacted]

响应详情

[redacted]