漏洞管理服务

最佳实践

文档版本	01
发布日期	2025-06-24

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 实践案例指引

表 1-1 服务最佳实践指引

实践	描述
使用漏洞管理服务扫描具有多种访问校验的网站	本实践主要介绍了如何扫描具有复杂访问机制的网站漏洞。
手动探索文件录制指导	本实践提供了手动探索文件录制指导。
使用漏洞管理服务进行局域网主机扫描	本实践介绍了如何使用使用CodeArts Inspector服务对内网主机进行扫描。
通过流水线自动完成CodeArts制品产物漏洞扫描	本实践主要介绍了通过搭建流水线，实现从代码仓到获取软件漏洞结果的整个流程，同时可以通过配置不同的准出条件，对漏洞实现分级管理。

2 使用漏洞管理服务扫描具有多种访问校验的网站

场景说明

如果用户的网站“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），请设置“cookie登录”方式进行网站漏洞扫描，以便CodeArts Inspector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**

约束限制

扫描报告仅支持专业版及以上版本扫描任务下载，如需下载，请升级到专业版及以上版本体验。

前提条件

已添加域名并完成域名认证。有关添加域名和域名认证的详细操作，请参见**添加待漏洞扫描的网站**。

步骤 1：获取网站的 cookie 值

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**。

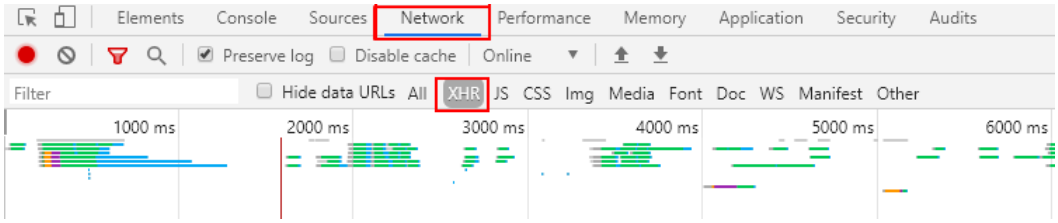
以Google Chrome浏览器为例说明，获取网站的cookie值的步骤如下：

步骤1 打开Google Chrome浏览器。按“F12”，进入浏览器的开发者模式。

步骤2 在地址栏中输入目标网站地址“www.example.com”。

步骤3 在调试页面中，选择“Network > XHR”，如图2-1所示。

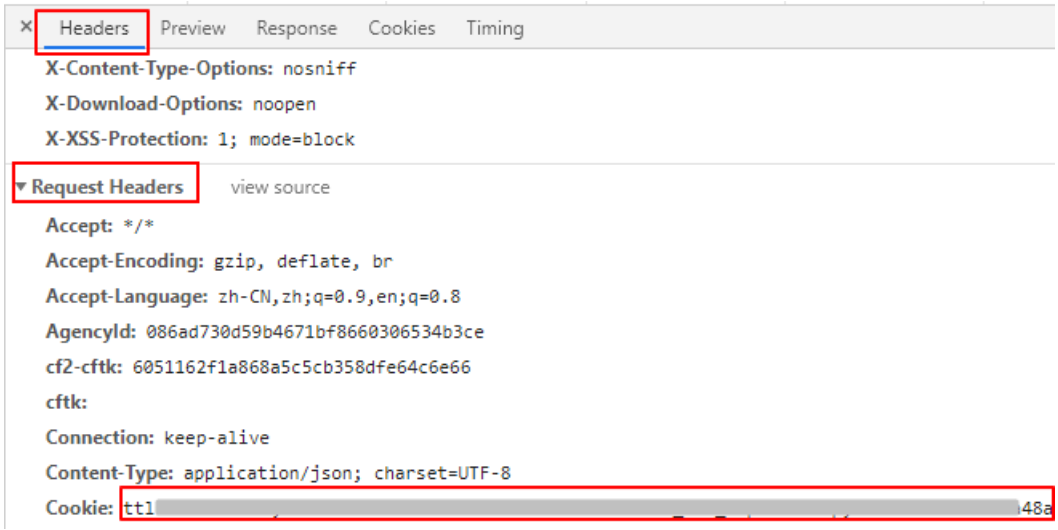
图 2-1 Network 页面



步骤4 在左侧导航树中，选择一个http请求。

步骤5 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2-2所示。

图 2-2 获取 cookie 值



----结束

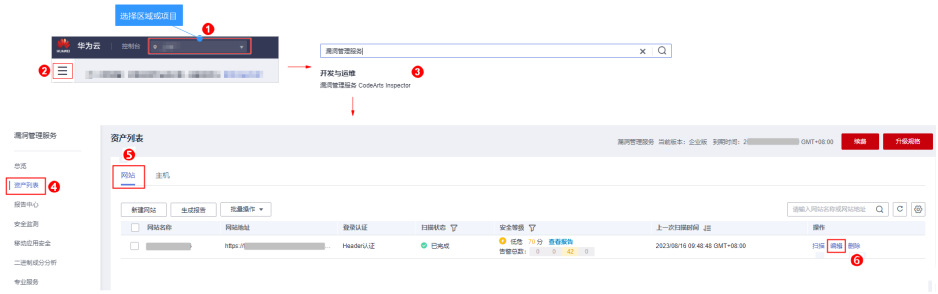
步骤 2：设置网站“cookie 登录”方式

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2-3所示。

图 2-3 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2-2中网站的cookie值完整复制到“cookie值”文本框中，如图2-4所示。

图 2-4 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，便于漏洞管理服务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

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”。

步骤2 在“创建任务”界面，根据扫描需求，设置扫描参数，如图2-5所示。

关于扫描项的详细介绍，请参见**创建扫描任务**。

图 2-5 创建扫描任务

步骤3 设置完成后，单击“确认”，进入扫描任务页面。

创建扫描任务后，会先进入“排队中”状态，满足运行条件后任务状态变为“进行中”。

说明

当网站列表中有“扫描状态”为“排队中”或“进行中”的任务时，可以单击网站列表上方的“批量取消”，在弹出的窗口中勾选需要取消扫描操作的网站进行批量取消。

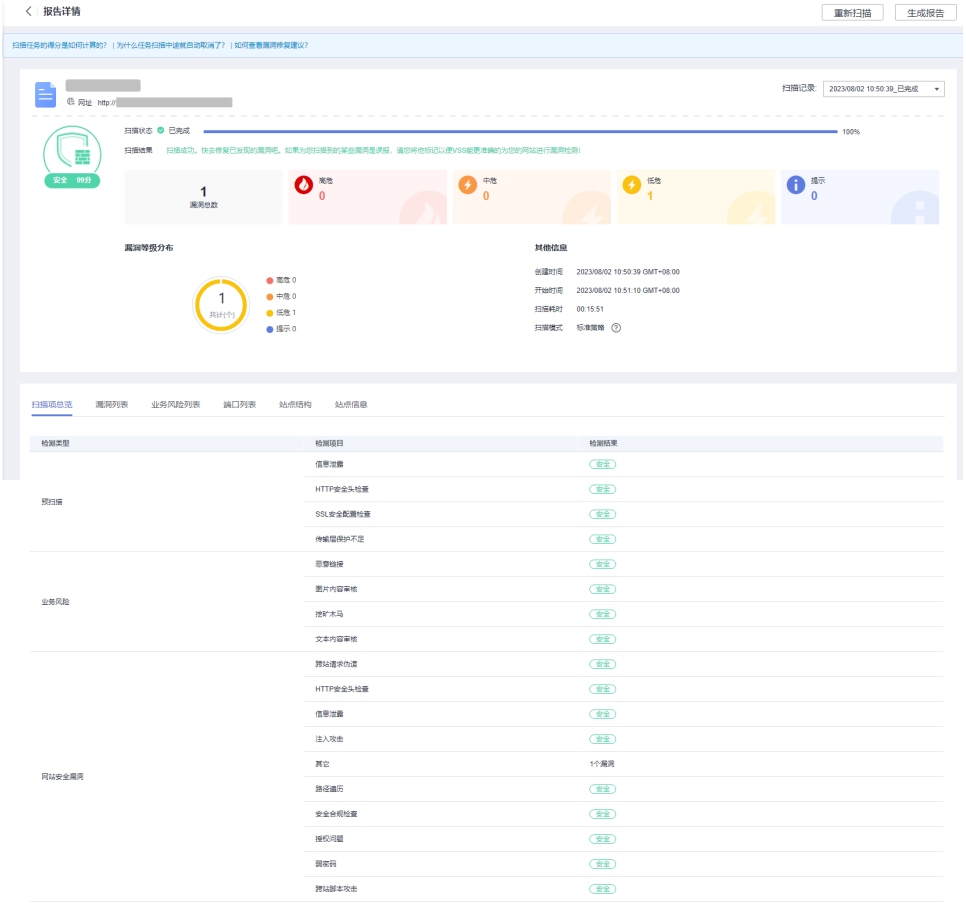
----结束

步骤 4：查看扫描结果并下载扫描报告

扫描任务执行成功后，您可以查看扫描结果并下载扫描报告。

步骤1 在目标网站所在行的“安全等级”列，单击“查看报告”，进入扫描任务详情页面，如图2-6所示。

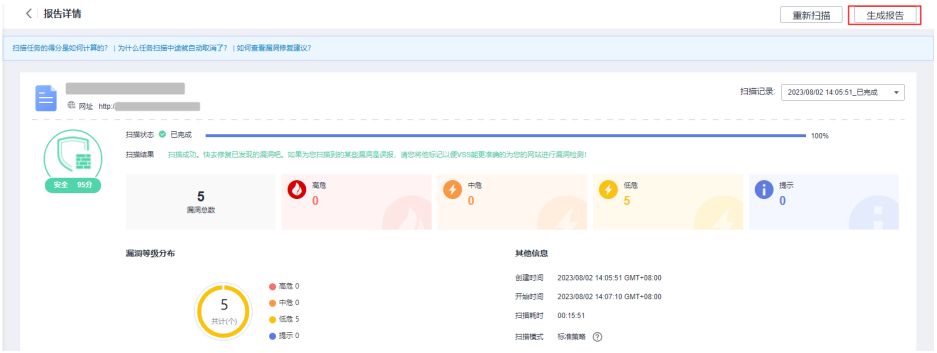
图 2-6 查看扫描任务详情



步骤2 单击“生成报告”，弹出“生成报告配置”窗口。

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。

图 2-7 生成扫描报告



步骤3 （可选）修改“报告名称”。

步骤4 单击“确定”，弹出前往报告中心下载报告的提示框。

步骤5 单击“确定”，进入“报告中心”页面。

步骤6 单击生成报告所在行的“下载”，可将报告下载到本地。

----结束

3 手动探索文件录制指导

目前CodeArts Inspector支持的手动探索文件格式为：BurpSuite site maps。
BurpSuite录制操作步骤如下。

安装

在官网下载社区版进行安装，具体参考：**Download Burp Suite Community Edition - PortSwigger**。

录制

步骤1 打开Burpsuite，选择Proxy。

步骤2 确认“Intercept”为“off”状态。

步骤3 单击“Open Browser”打开BurpSuite内置浏览器。

步骤4 在浏览器中访问Web应用，单击需要测试的界面。

步骤5 回到BurpSuite，单击“Target”。

步骤6 在“Site map”中选择Web应用对应的域名。

步骤7 右键选择“save selected items”保存xml文件。

----结束

操作录屏

具体内容请参考**手动探索文件录制指导**。

常见问题

- Https网站显示证书错误
  请上传浏览器信任的BrupSuite证书，具体请参考如下链接：
  Installing Burp's CA certificate in Chrome - PortSwigger
- Web应用开启HSTS
  How to Clear HSTS Settings on Chrome, Firefox and IE Browsers
- 多重代理/BurpSuite上层代理

Burp Suite Options: Upstream Proxy Servers - PortSwigger

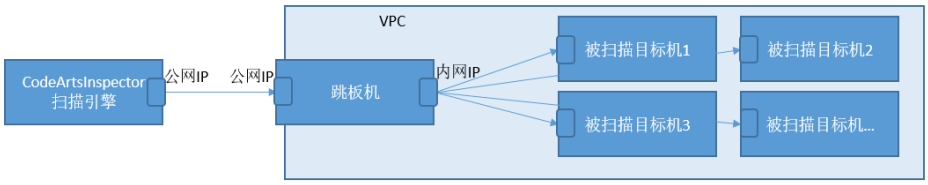
4 使用漏洞管理服务进行局域网主机扫描

约束限制

CodeArts Inspector服务通常对公网上可访问的主机进行漏洞扫描测试。该服务的扫描引擎出口公网IP地址：119.3.232.114、119.3.237.223、124.70.102.147、121.36.13.144、124.70.109.117、139.9.114.20和119.3.176.1。因此，被扫描的目标需要允许以上这些IP地址的访问。

场景说明

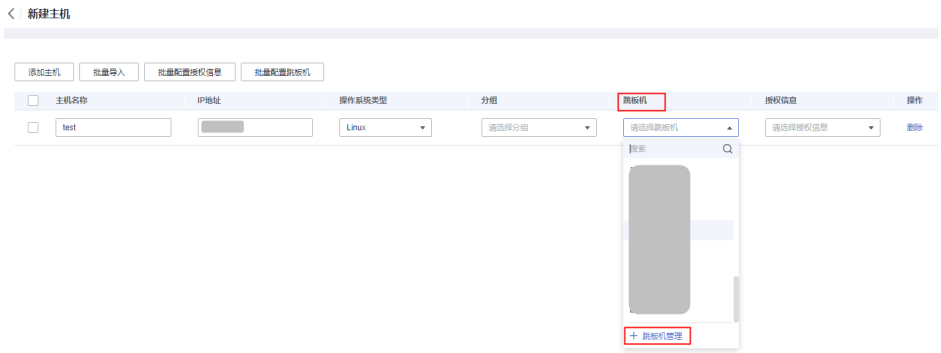
对于一些使用用户而言，用户的扫描目标主机部署在私有VPC中，没有公网IP地址，这使得CodeArts Inspector服务的扫描引擎无法直接访问这些目标主机。为了实现对这类内网主机的漏洞扫描，我们提出了如下组网解决方案。该方案需要使用一台配置了双IP地址的跳板机（跳转服务器），其中一个IP地址是公网IP，能够与扫描引擎通信；另一个IP地址位于内网中，用于与被扫描的目标主机互通。通过这种方式，我们能够建立从扫描引擎到被扫描目标主机的网络连接，进而完成内网主机的漏洞扫描。



步骤1 创建主机扫描任务。在IP地址栏填写被扫描目标机的内网IP。

步骤2 添加跳板机配置。

配置的跳板机“公网IP”需要放通扫描引擎侧的公网IP（允许访问），跳板机的内网IP需要与被扫描目标机的内网环境互通。



步骤3 检查跳板机上配置文件。

添加跳板机后，需要检查跳板机上的ssh配置文件。“/etc/ssh/sshd_config”中存在AllowTcpForwarding yes的配置，用于支持SSH授权登录。修改配置后需重启sshd服务。 配置完成后可以执行命令 “sshd -T 2>/dev/null |grep allowtcpforwarding”检查是否配置成功。

```
[root@localhost ~]# sshd -T 2>/dev/null |grep allowtcpforwarding
allowtcpforwarding yes
```

----结束

验证

跳板机及被扫描对象的认证信息配置完成后可以单击“互通性”按钮验证认证信息配置的准确性。 如果不成功，可以按提示的信息（如：网络不通、密码不正确等）进行问题排查和修复。 如果成功，即可启动扫描。

5 通过流水线自动完成 CodeArts 制品产物漏洞扫描

应用场景

随着软件功能的不断扩大，网站面临的安全风险也在增加，如何快速精准地识别网站安全风险成了一大难题。

通过搭建流水线，可实现从代码仓到获取软件漏洞结果的整个流程，同时可以通过配置不同的准出条件，对漏洞实现分级管理。

方案优势

- 搭建简单，无需重复配置

  只需在搭建流水线时配置一次，即可重复实现完成漏洞扫描的完整流程。
- 漏洞风险分级治理

  支持配置准出条件，实现对不同风险等级漏洞的分级管理并对扫描结果进行拦截。

约束限制

流水线可配置定时任务或外部触发执行，使用插件扫描会扣除用户所购买的套餐配额，如未购买套餐，则扣除免费的基础版配额。

操作流程

本文介绍如何通过流水线完成代码修改、漏洞扫描的全过程，基本操作流程如下：

步骤1：新建规则和策略

步骤2：新建Scrum项目

步骤3：新建代码仓库

步骤4：新建流水线

步骤5：查看插件执行结果

步骤 1：新建规则和策略

步骤1 登录华为云官网，单击页面右上角“**控制台**”。

步骤2 在页面左上角单击☰，打开服务列表。

步骤3 搜索“**流水线**”。

步骤4 单击“**流水线 CodeArts Pipeline**”，进入流水线服务首页。

步骤5 单击右上角头像图标，在下拉菜单中选择“**租户设置**”，进入租户设置页面。

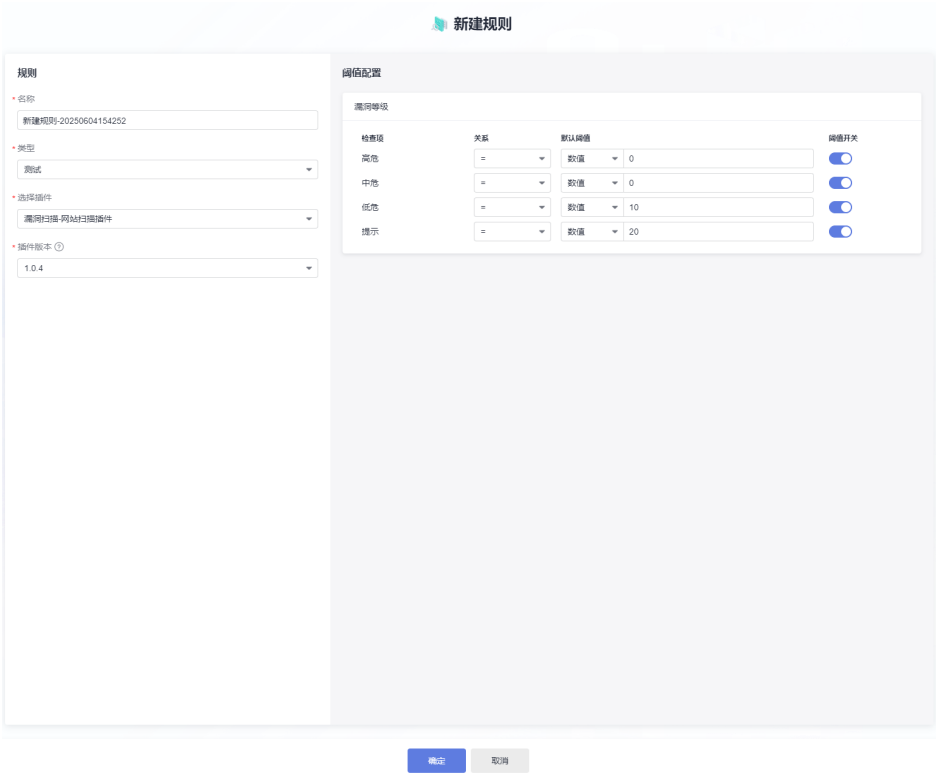
步骤6 单击左侧导航“**策略管理 > 规则**”，进入规则管理页面。

步骤7 单击“**新建规则**”，进入“**新建规则**”页面，配置以下信息。

表 5-1 配置规则信息

参数项	说明
名称	规则名称，使用自动生成的即可。
类型	规则类型，选择“**测试**”。
选择插件	规则绑定的插件名称，选择“**漏洞扫描-网站扫描插件**”。
插件版本	规则绑定的插件版本（选择插件的最新版本），不同插件版本输出的阈值可能有差异，例如选择“**1.0.5**”。
阈值配置	配置检查项阈值，例如图5-1所示。

图 5-1 新建规则



步骤8 单击“**确定**”，完成规则创建。

步骤9 单击左侧导航“**策略**”，进入策略管理页面。

步骤10 单击“**新建策略**”，进入“**新建策略**”页面，输入策略名称，勾选新建好的规则。

图 5-2 新建策略

步骤11 单击“**确定**”，完成策略创建。

----结束

步骤 2：新建 Scrum 项目

步骤1 单击顶部导航栏“**首页**”。

步骤2 在所有项目下单击“**Scrum > 新建项目**”。

步骤3 选择“**Scrum**”项目模板，单击“**选用**”，进入新建项目页。

步骤4 项目名称填写“**Scrum01**”，其它保持默认即可。

步骤5 单击“**确定**”后，进入到“**Scrum01**”项目下。

----结束

步骤 3：新建代码仓库

步骤1 在页面导航栏选择“**代码 > 代码托管**”，进入代码托管页面。

步骤2 单击“**新建仓库**”，选择“**普通新建**”。

步骤3 单击“**下一步**”，填写仓库名称。

步骤4 单击“**确定**”，完成代码仓库的创建。

----结束

步骤 4：新建流水线

步骤1 在页面导航栏选择“**持续交付 > 流水线**”，进入流水线页面。

步骤2 单击“**新建流水线**”，根据需要配置流水线信息。

1. 基本信息：配置以下信息，单击“**下一步**”。

表 5-2 流水线基本信息

配置项	配置建议
名称	流水线名称，使用默认生成的即可。
代码源	选择“Repo”。
代码仓	选择**已创建的代码仓库**。
默认分支	选择“master”分支。

2. 选择模板：选择**“空模板”**，单击**“确定”**。

步骤3 进入**“任务编排”**页面，系统默认生成两个阶段（“流水线源”和“阶段_1”）。

1. **流水线源**

   保持默认即可。

2. **阶段_1**（扫描阶段）

   a. 单击**“阶段_1”**阶段的**“新建任务 > 从空任务新建”**，弹出新建任务侧滑框。

   b. 单击**“测试”**分类，找到**“漏洞扫描-网站扫描插件”**插件。

   c. 将鼠标移动到插件，单击**“添加”**，扫描域名配置想要扫描的域名。

   d. 单击**“确定”**，完成任务配置。

   e. 单击**“阶段_1”**阶段的“准出条件”，在弹出的侧滑框里添加准出条件，将鼠标移动到**“标准策略准出条件”**上，单击**“添加”**，并选择**已创建好的策略**。

   f. 单击**“确定”**，完成准出条件配置。

步骤4 任务编排完成后，单击**“保存并执行 > 执行”**，开始执行流水线。

----结束

步骤 5：查看插件执行结果

步骤1 流水线执行完成后，进入详情页面。

步骤2 单击**“阶段_1”**阶段的**“漏洞扫描”**任务，弹出侧滑框。

步骤3 在侧滑框的**“任务日志”**页面，单击**“详情”**，页面跳转到漏洞扫描服务对应的扫描详情页面，即可查看扫描结果。

步骤4 在侧滑框的**“任务结果”**页面，单击**“漏洞扫描-网站扫描插件”**可以直接查看部分扫描结果。

步骤5 单击准出条件，可查看扫描结果是否满足设置的规则，从而控制流水线执行。

- 当扫描结果满足条件时，流水线继续执行。
- 当扫描结果不满足条件，流水线停止执行。

----结束

