# 漏洞管理服务

# 最佳实践

**文档版本** 01

**发布日期** 2024-06-06

**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 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**

## 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**添加域名完成**。

## 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。

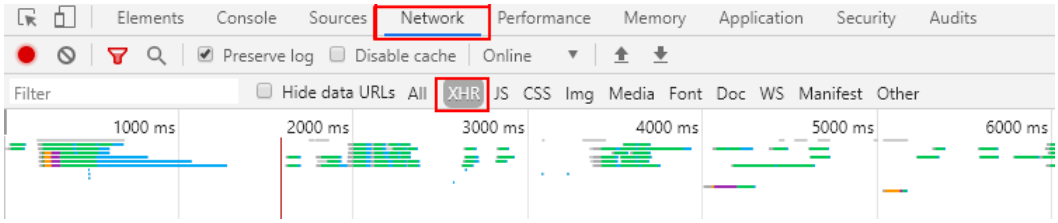
**步骤2** 按“F12”，进入浏览器的开发者模式。

**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1-1**所示。

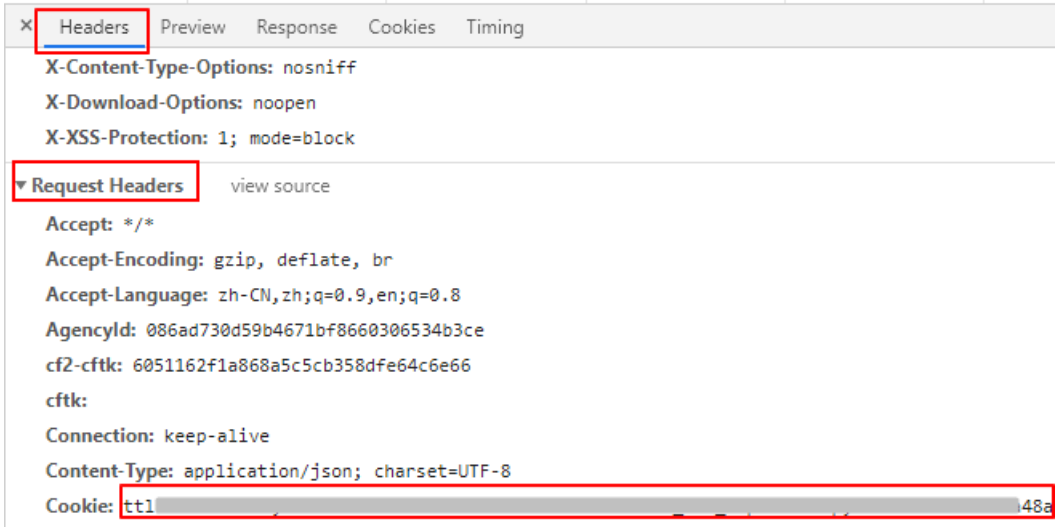
**图 1-1** Network 页面




**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1-2所示。

**图 1-2** 获取 cookie 值




**----结束**

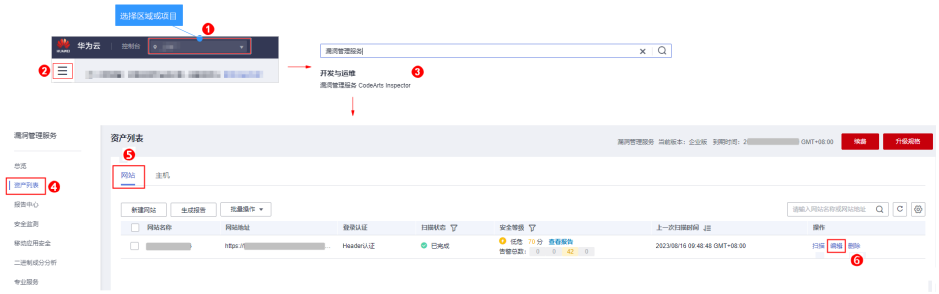
## 步骤 2：设置网站“cookie 登录”方式

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1-3所示。

**图 1-3** 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1-2中网站的cookie值完整复制到“cookie值”文本框中，如图1-4所示。

**图 1-4** 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

**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”。

**步骤2** 在“创建任务”界面，根据扫描需求，设置扫描参数，如图1-5所示。

关于扫描项的详细介绍，请参见**创建扫描任务**。

**图 1-5** 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。

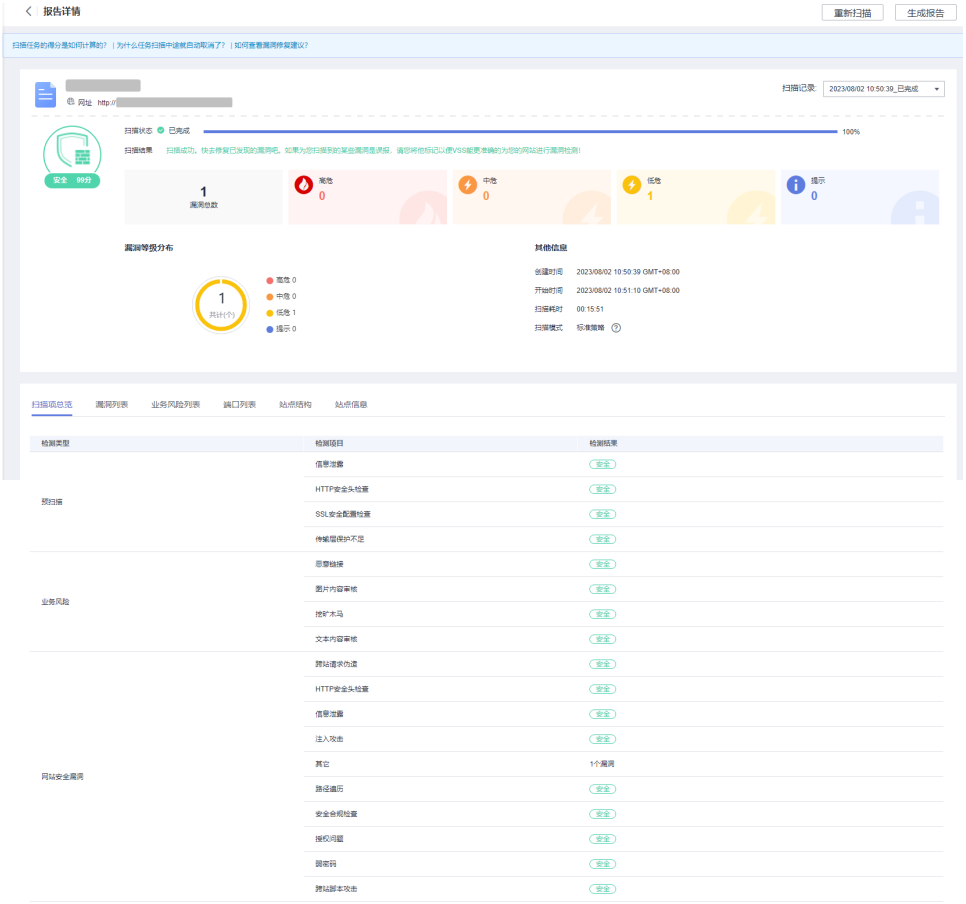
**----结束**

## 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1-6所示。

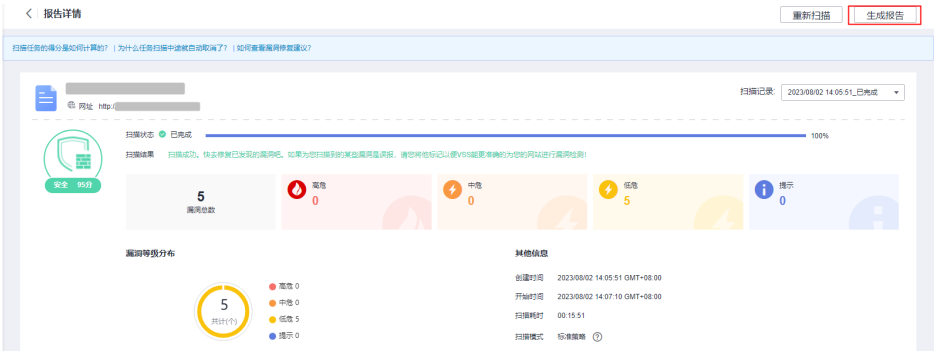
**图 1-6** 查看扫描任务详情




**步骤2** 单击“生成报告”，弹出“生成报告配置”窗口。

扫描报告仅支持专业版及以上版本扫描任务下载，请升级到专业版及以上版本体验。

**图 1-7** 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**

# 2 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

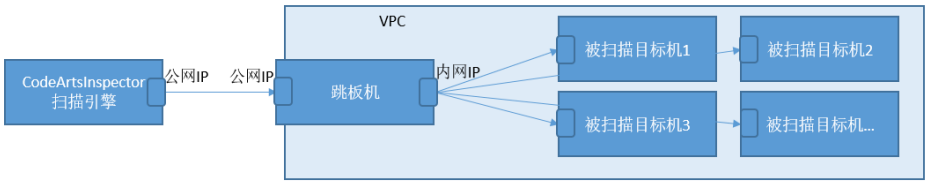
**Burp Suite Options: Upstream Proxy Servers - PortSwigger**

# 3 使用 CodeArts Inspector 服务对内网主机进行扫描

## 场景说明

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地址包括：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。

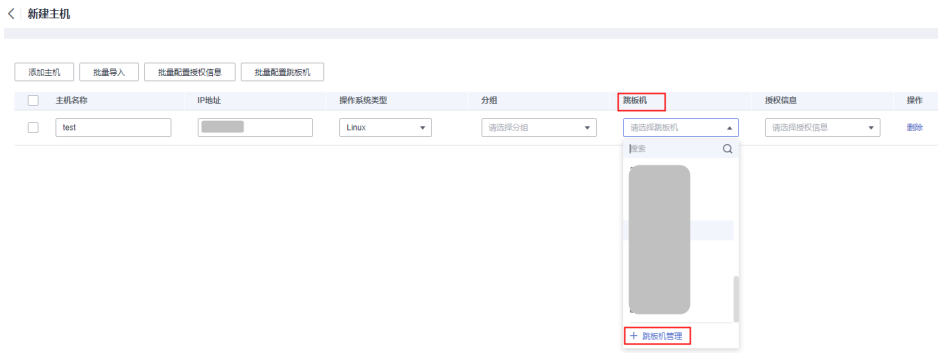
然而，对于一些客户而言，他们的扫描目标主机部署在私有VPC中，没有公网IP地址，这使得CodeArts Inspector服务的扫描引擎无法直接访问这些目标主机。为了实现对这类内网主机的漏洞扫描，我们提出了如下组网解决方案。该方案需要使用一台配置了双IP地址的跳板机（跳转服务器），其中一个IP地址是公网IP，能够与扫描引擎通信；另一个IP地址位于内网中，用于与被扫描的目标主机互通。通过这种方式，我们能够建立从扫描引擎到被扫描目标主机的网络连接，进而完成内网主机的漏洞扫描。




**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授权登录转发。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点击“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。

# A 修订记录

| 发布日期 | 修改说明 |
| --- | --- |
| 2024-06-06 | 第五次正式发布。<br>新增使用CodeArts Inspector服务对内网主机进行扫描。 |
| 2023-09-07 | 第四次正式发布。<br>1. 资产列表页面优化。<br>2. “漏洞扫描服务 VSS”更名为“漏洞管理服务 CodeArts Inspector”。 |
| 2021-07-13 | 第三次正式发布。<br>删除通过VSS扫描内网网站。 |
| 2020-05-21 | 第二次正式发布。<br>新增通过VSS扫描内网网站。 |
| 2019-11-07 | 第一次正式发布。 |