#### 漏洞管理服务

最佳实践

文档版本01发布日期2025-01-20





#### 版权所有 © 华为云计算技术有限公司 2025。保留一切权利。

非经本公司书面许可,任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部,并不得以任何形式传播。

#### 商标声明

NUAWE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: <u>https://www.huaweicloud.com/</u>

目录

1	实践案例指引	. 1
2	使用漏洞管理服务扫描具有多种访问校验的网站	.2
3	手动探索文件录制指导	.8
4	使用漏洞管理服务进行局域网主机扫描1	10



#### 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。

### 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<mark>添加待漏</mark> 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

× Headers Preview Response Cookies Timing						
X-Content-Type-Options: nosniff						
X-Download-Options: noopen						
X-XSS-Protection: 1; mode=block						
• Request Headers view source						
Accept: */*						
Accept-Encoding: gzip, deflate, br						
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8						
Agencyld: 086ad730d59b4671bf8660306534b3ce						
cf2-cftk: 6051162f1a868a5c5cb358dfe64c6e66						
cftk:						
Connection: keep-alive						
Content-Type: application/json; charset=UTF-8						
Cookie: tt1 44	8a					

----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

	选择区域或项目						
# 华为云 2 三	: 22416 •		展向管理服务 开发与运输 原向管理服务 CodeArts Inspects	<b>8</b>		×Q	
			÷.				
還同管理服务	资产列表					属两营理报号 尚能版本: 企业版 多隅时间: 2	CMT+08:00 统器 升级规图
55 21-718 <b>4</b>	网站主机						
报告中心·	#187% ±138%	抗量操作 *					INALARSENIERISE Q C
安全监罚	网站名称	网络地址	强荣认证	日間秋念 ▽	安全等级 🎖	上一次扫描时间 1日	操作
移动应用安全		https://j	Headeri), i <u>E</u>	<ul> <li>B完成</li> </ul>	○ 任他 70分 查查报告 告偿已款: 0 0 42 0	2023/08/16 09:48:48 GMT+08:00	1315 (ANM) 8500
二进制成分分析							6
专业服务							

 $\sim$ 

**步骤3** 在弹出的"编辑"对话框中,将<mark>图2-2</mark>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	t
----------	--------	------	---

编辑网站	
网站信息	
网站地址	http://www.test.com
网站名称	test
Web页面登录	
Cookie登录	
如何获取网站cookie	值?
★ cookie值	Ø
Header登录	
网站登录验证	
輸入一个登录成功后	才能访问的网址,便于CodeArts Inspector快速判断您的登录信息是否有效。
验证登录网址	

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 创建任务

基础版、专业版、高	级版及企业版有何2	∑别? 网站漏洞扫描	一次需要多	次?	×
真写扫描信息					
开始时间	请选择日期时间		⊞		
★ 扫描策略	标准策略		•	0	
手动探索文件	点击右侧按钮先	添加再上传		添加文件	?
是否扫描登录URL	0				
日描项设置					
扫描项		操作			
Web常规漏洞扫描(	包括XSS、SQL				
端口扫描					
弱密码扫描					
CVE漏洞扫描					
网页内容合规检测 (]	文字)				
网页内容合规检测 (問	图片)				
网站挂马检测					
				确认	取消

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<mark>图2-6</mark>所示。

#### 图 2-6 查看扫描任务详情

く 报告详情					重新扫描	生成报告
扫描任务的得分最如何计算的?  为什么任务	月扫描中途就自动取消了?   如何 <b>查看满</b> 两修复建议	0				
<ul> <li>● 网社 http://</li> <li>日期は</li> </ul>	5 • 已完成 第 日田成功、快去排發已發現的運行吧。 20第2	SERFOXERRER, WORKSCH	IVSS版更重编的为您的网站进行集	962801	 推进记录: 2023/08/02 10: 100%	50:39_已完成 -
安全 99 <del>万</del>	1 展示地政	0			<b>1</b> <sup>揭示</sup> 0	
ative de	250分布 1 1 1 1 1 1 1 1 1 1 1 1 1		其代代统 创建型月 开始时间 扫描模型	2         2023/08/02 19:50 39 0/MT+08:00           3         2023/08/02 19:51 10 0/MT+08:00           4         00 15:51           2         56:88888		
扫描项总元 漏洞列表	业务风险列表 编口列表 站点结	构 站点信息				
检测类型		检测项目		检测结果		
		信息过露		(安全)		
预扫描		HTTP安全头检查		(安全)		
		SSL安全配置检查		安全		
		传输层保护不足		安全		
		思意始接		( <u>*</u> *		
业务风险		图片内容审核		(安全)		
		挖矿木马				
		文本内容東核				
		信用注题		(14) (14)		
				(安全)		
		其它		1个雇用		
同站安全尾洞		路径違历		( <u>\$</u> \$		
		安全合规检查		(1911) (1912)		
		接段问题		( <u>\$</u> \$		
		調密码		<u>*</u>		
		跨站副本攻击		( 全 室)		

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

く 报告详情									I	新扫描	生成报告
扫描任务的得分是如何计算的?   7	为什么任务扫描中途就自动取得了?  如何重要系	周修叙建议?									
								1	1描记录: 2023	08/02 14:05:51_	巴兆成 ▼
	扫描状态 ♥ 已完成	9 <b>6。</b> 如果为您扫描到的某些赢得	同星误报,请您将他标记以	以使VSS能更准确的)	为您的网站进行漏	1982-1991				100%	
安全 95分	<b>5</b> 通用处数					3	低電 5		<b>1</b> 提示 0		
	漏调等级分布				其他信息						
		<b>憲</b> 意 0			<ul><li> () 通知1日 21 () 1日 21 () 1日 21 () 1日 21 </li></ul>	23/08/02 14:05:5	I GMT+08:00				
	5 <sup>共计(个)</sup>	● 中他 0 ● 低饱 5 ■ 提示 0			<ul><li>13回転町 01</li><li>13回載載式 65</li></ul>	2:15:51	- GWH - 992,00				

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。 く新建主机

激加主机 批量导入	北量配置接权信息 批量配置期版机					
主机名称	IP地址	操作系统类型	分組	35665491	授权信息	操作
			Interface and the second second		Sectors (10) and (10) and (20)	
test		Linux 👻	请选择分组	▼ 第达控制版机 ▲	销达洋技权信息	* #150x
				搜索 C		
				+ 跳版机管理		

#### 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。

产列表	● 互適性別式成功 ×
网站 主机 API	
□ 主机名称 19地址 接段信息 数板机 分組 主机连接线态 ♡ 扫描状态 ♡ 安全等级 ♡	上一次扫描时间 🖯 操作
_ 171 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	扫描 编4 互通性 影除