



漏洞扫描服务

用户指南

文档版本 03

发布日期 2019-07-12

华为技术有限公司



版权所有 © 华为技术有限公司 2019。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



HUAWEI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，华为公司对本文档内容不做任何明示或默示的声明或保证。

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。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编： 518129

网址： <http://e.huawei.com>

目录

1 开通 VSS.....	1
1.1 版本规格功能说明.....	1
1.2 购买漏洞扫描服务.....	2
2 一键扫描.....	5
3 一键风险识别.....	7
4 资产列表.....	10
4.1 查看资产列表.....	10
4.2 添加域名.....	11
4.3 域名认证.....	12
5 任务列表.....	15
5.1 创建扫描任务.....	15
5.2 查看扫描详情.....	18
6 总览.....	22
6.1 查看扫描概况.....	22
6.2 漏洞列表.....	24
6.2.1 查看漏洞列表.....	24
6.2.2 查看漏洞详情.....	25
6.2.3 标记为忽略.....	26
A 修订记录.....	28

1 开通 VSS

1.1 版本规格功能说明

漏洞扫描服务提供基础版扫描服务和专业版扫描服务，基础版可免费使用，但是功能和规格受限，专业版需付费，具体功能和规格对比如表1-1所示。

表 1-1 功能/规格说明

版本	付费模式	功能	规格
基础版	免费	<ul style="list-style-type: none">● 漏洞检测● 重新扫描● 定时扫描● 端口扫描● 自定义登录方式● Web 2.0 高级爬虫扫描	<ul style="list-style-type: none">● 域名个数：5 个● 扫描次数：单日 5 次● 单个任务时长：2 小时● 任务优先级：低
专业版	付费	<ul style="list-style-type: none">● 漏洞检测● 重新扫描● 定时扫描● 端口扫描● 自定义登录方式● Web 2.0 高级爬虫扫描● 任务完成后短信通知用户● 查看修复建议● 下载扫描报告● 弱密码扫描	<ul style="list-style-type: none">● 域名个数：按需购买● 扫描次数：单个域名每月可扫描 60 次● 单个任务时长：无限制● 任务优先级：高

1.2 购买漏洞扫描服务

该任务指导用户购买漏洞扫描服务的专业版扫描功能。如果您是新用户，请首先完成预扫描，详细操作步骤见《漏洞扫描服务用户指南》的“一键扫描”章节，然后按照操作步骤完成购买。

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 选择“安全 > 漏洞扫描服务 > 资产列表”，进入“资产列表”界面。

步骤3 在界面右上角，单击“购买专业版”。

说明

也可以通过选择“安全 > 漏洞扫描服务 > 总览”，进入“总览”界面，单击“购买专业版”，进入“购买漏洞扫描服务”界面。

步骤4 在购买漏洞扫描服务界面，根据表1-2进行服务选型配置，如图1-1和图1-2。

图 1-1 服务选型-基础版

The screenshot shows a web interface for selecting a service plan. At the top, there are three steps: 1. 服务选型 (Service Selection), 2. 订单确认 (Order Confirmation), and 3. 付款 (Payment). The main content area is titled '规格' (Specifications) and includes the following elements:


- 规格选择:** Two radio buttons are present: '基础版 (免费)' (Basic Edition (Free)) which is selected, and '专业版' (Professional Edition).
- 规格说明:** A list of features for the basic edition:
 - 支持OWASP、WASC等常见漏洞检测
 - 可自定义扫描检测强度、扫描爬虫等设置
 - 支持登录扫描，多种登录方式可选择
 - 支持定时扫描，避开网站业务高峰
 - 支持高危端口扫描，提升服务器安全
 - 动态调整扫描压力，保证业务可用性
 - 未域名认证时可对部分项进行快速扫描
- 温馨提示:** 基础版每日扫描次数上限为5次；单次扫描任务时限2小时，可完成中小型网站的一次扫描，如果您的网站过大，建议您购买专业版。
- 配置:** A section with a dropdown menu for '域名/IP地址' (Domain/IP Address) showing 'http://' and an input field for '请输入IP或域名' (Please enter IP or domain).

At the bottom left, it says '配置费用 免费' (Configuration fee: Free). At the bottom right, there is a red button labeled '立即体验' (Experience Now).

图 1-2 服务选型-专业版



表 1-2 服务选型参数说明

参数	参数说明
规格选择	目前仅“专业版”需要付费，“基础版”可免费使用。
购买时长	可以选择1个月~1年的时长。
域名数量	配置的“域名/IP地址”个数。
域名/IP地址	配置需要进行漏洞扫描的域名。单击  可以添加多个域名。 <ul style="list-style-type: none"> ● 基础版一次只能配置一个域名 ● 专业版每次最多可配置10个域名

步骤5 参数设置完毕后，在页面右下角，单击“立即购买”。

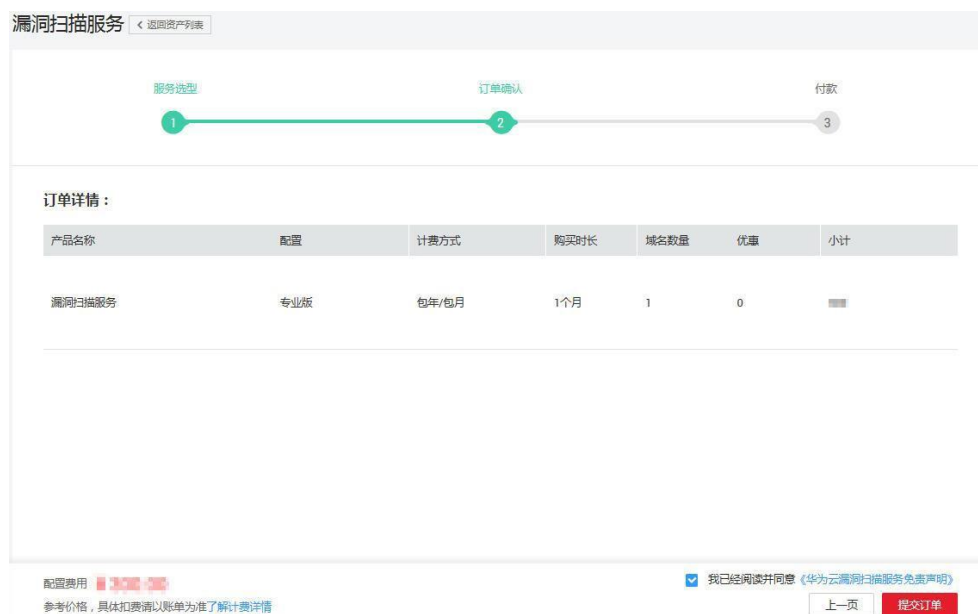
 **说明**

如果您对价格有疑问，可以单击“了解计费详情”了解产品价格。

步骤6 确认订单详情无误并阅读《华为云漏洞扫描服务免责声明》后，勾选“我已阅读并同意《华为云漏洞扫描服务免责声明》”，单击“提交订单”。

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。

图 1-3 订单确认



步骤7 在“付款”页面，选择付款方式进行付款。

----结束

2 一键扫描

该任务指导新用户免费体验漏洞扫描服务。

操作步骤

步骤1 输入想要扫描的域名/IP 地址，如图 3-1，单击“开始扫描”进入“正在扫描”界面。

图 2-1 新用户体验界面



步骤2 您可以查看扫描进度，如图2-2。

图 2-2 正在扫描



步骤3 扫描完成后单击界面右上角“专业全面的漏洞扫描服务，点击免费试用”进入“资产列表”界面完成域名认证，也可以通过单击页面下方的“立即进行域名认证”按钮来进行域名认证，如图3 扫描详情所示，各栏目说明如表1 扫描结果说明所示。

图 2-3 扫描详情

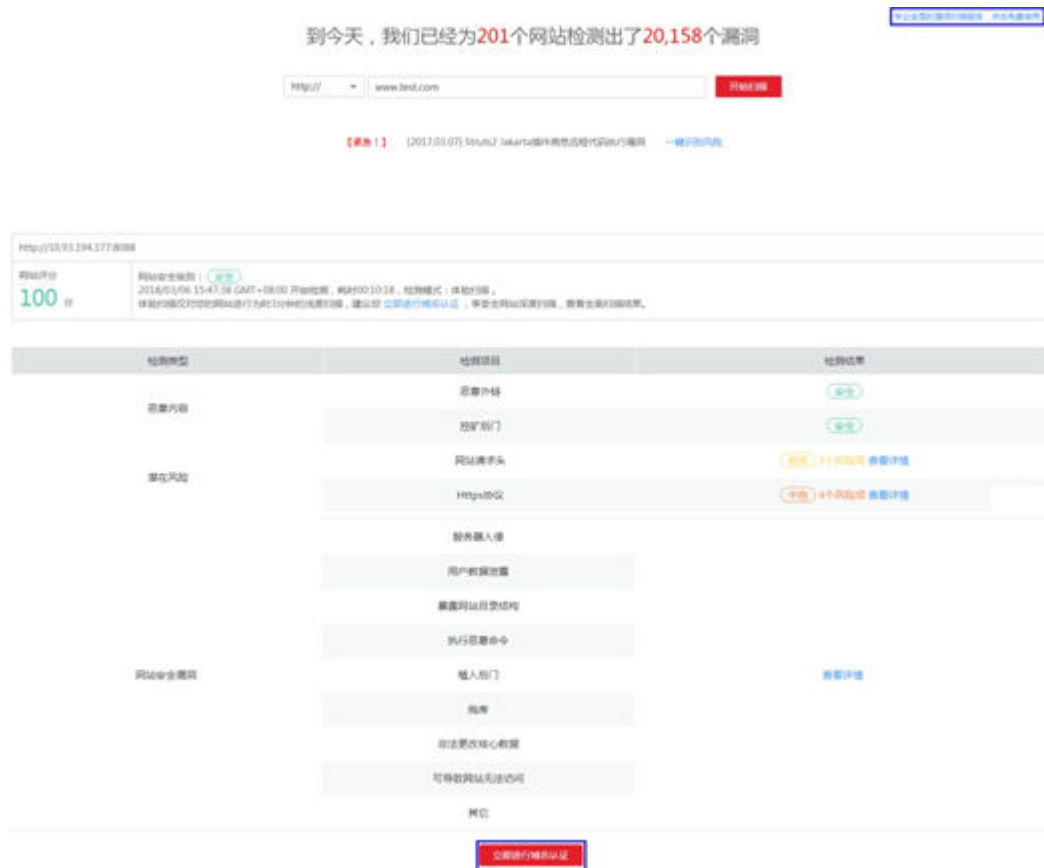


表 2-1 扫描结果说明

栏目	说明	操作
检测类型	对扫描结果进行分类显示。	-
检测项目	显示扫描的项目，属于检测类型的子类。	-
检测结果	显示漏洞扫描的结果	<ul style="list-style-type: none"> ● 结果为安全显示 安全。 ● 有风险会显示相应的风险级别，单击“查看详情”查看具体的漏洞信息，如 低危 5个风险项 查看详情。

----结束

3 一键风险识别

该任务指导新用户免费体验最新紧急漏洞扫描。

老用户可以通过“安全>漏洞扫描服务>总览”的最新漏洞新闻单击“一键检测”使用此功能。

操作步骤

- 步骤1** 单击“一键风险识别”进入“一键检测最新紧急漏洞风险”界面，如[图1 一键风险识别](#)和[图2 一键检测最新紧急漏洞风险](#)。

图 3-1 一键风险识别



图 3-2 一键检测最新紧急漏洞风险

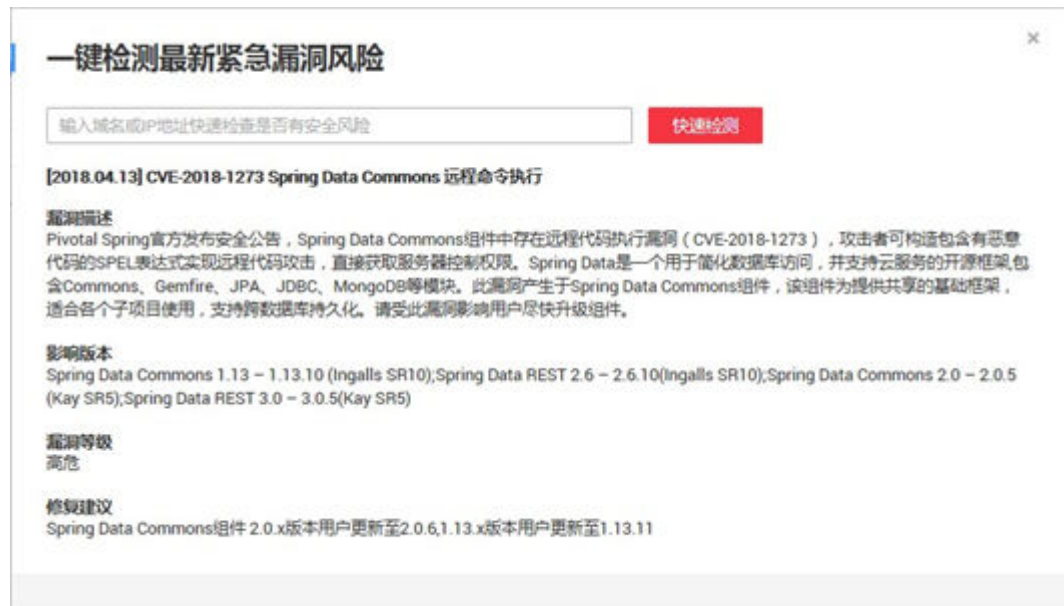


表 3-1 漏洞风险说明

栏目	说明
漏洞描述	描述当前紧急漏洞的基本内容和风险。
影响版本	此漏洞影响的版本。
漏洞等级	此漏洞的危害等级。
修复建议	给出的修复建议。

步骤2 输入您的域名或 IP 地址，单击“快速检测”。

步骤3 完成检测后，如果存在该风险，请单击“立即进行域名认证”或者单击页面下方的“立即进行域名认证”来完成域名认证（具体操作请参见[域名认证](#)），对您的网站进行更深层次的漏洞扫描。

图 3-3 紧急漏洞检测结果

一键检测最新紧急漏洞风险 [查看详情](#)

网站风险级别	检测网站	http://www.test.com
安全	网站域名信息	IP: unknown 框架: unknown 网站服务器: unknown
	温馨提示	本次提交的最新CVE漏洞信息有可能对您的网站造成危害，建议您 立即进行域名认证 对网站进行更全面深入的漏洞扫描服务，保障网站安全。

【2018.04.12】CVE-2018-1273 Spring Data Commons 远程命令执行	
漏洞编号	CVE-2018-1273
漏洞描述	Privatall Spring官方发布安全公告，Spring Data Commons组件中存在远程代码执行漏洞（CVE-2018-1273），攻击者可构造包含恶意代码的SPEL表达式以篡改代码执行，直接获取服务器控制权。Spring Data是一个用于简化数据库访问，并支持云服务的开源框架，包含Commons、Gemfire、JPA、JDBC、MongoDB等模块。此漏洞产生于Spring Data Commons组件，该组件为提供共享的基础框架，适合各个子项目使用，支持数据库持久化。请参见漏洞详情/用户升级组件。
受影响版本	Spring Data Commons 1.13 - 1.13.10 (Ingress SR10); Spring Data REST 2.6 - 2.6.10 (Ingress SR10); Spring Data Commons 2.0 - 2.0.5 (Kay SR5); Spring Data REST 3.0 - 3.0.5 (Kay SR5)
漏洞等级	高危
修复建议	Spring Data Commons(组件 2.0.x版本)更新至2.0.6,1.13.x版本)更新至1.13.11

---结束

4 资产列表

4.1 查看资产列表

该任务指导用户查看资产列表。

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 > 资产列表”，进入“资产列表”界面，如图1 资产列表所示，相关参数说明如表1 资产列表参数说明所示。

说明

- 用户可以单击操作列的“更多”，编辑、扫描或删除域名。
- 如果该域名是专业版，必须显示“已过期”才能删除。

图 4-1 资产列表



资产信息	扫描状态	操作
http://115.53.194.177:8088 资产版本：基础版 到期时间：2018-04-01 23:59:59	100分 时间：2018/03/29 17:08 高危0个，中危0个，低危0个，漏洞0个	马上扫描 更多+
http://www.0204.com 资产版本：基础版 到期时间：2018/03/29 23:59:59	0分 时间：- 高危0个，中危0个，低危0个，漏洞0个	继续认证 更多+
http://182.252.192.100 资产版本：专业版 到期时间：2018/05/29 23:59:59	83分 时间：2018/05/29 21:56:41 高危0个，中危1个，低危4个，漏洞0个	马上扫描 更多+

表 4-1 资产列表参数说明

参数	参数说明
域名信息	<ul style="list-style-type: none">● 域名/IP 地址和认证状态<ul style="list-style-type: none">- 已认证 目标域名已完成域名认证。可以单击操作列的“马上扫描”创建扫描任务，具体操作请参见 创建扫描任务。- 未认证 目标域名未完成域名认证。可以单击操作列的“前往认证”进行域名认证，具体操作请参见 域名认证。- 已过期 若专业版超过购买时长时，将会显示为“已过期”。单击“重新购买”可对该域名进行续费，具体操作请参见《漏洞扫描服务 购买指南》。● 任务名称● 套餐版本：当前使用的漏洞扫描版本，“基础版”或“专业版”。● 到期时间：<ul style="list-style-type: none">- 当用户使用“基础版”时，显示到期日期。- 当用户使用“专业版”时，显示到期日期；若使用套餐已过期，可单击“重新购买”。
最新扫描情况	域名最近一次扫描任务的信息，包括得分、扫描时间和各等级的漏洞数量。

---结束

4.2 添加域名

该任务指导用户添加域名。

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** 选择“安全 > 漏洞扫描服务 > 资产列表”，进入“资产列表”界面。
- 步骤3** 单击“新增域名”或“添加新域名”，如 [图 7-2](#) 所示。

图 4-2 新增域名



步骤4 单击“确认新增”，新增域名成功。进入“域名认证”页面，具体参见[域名认证](#)。

说明

用户也可以直接通过“购买服务”添加域名。

----**结束**

4.3 域名认证

该任务指导用户对已添加的域名进行域名认证。

前提条件

- 已获取管理控制台的登录账号与密码。
- 域名状态为“未认证”。

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 > 资产列表”，进入“资产列表”界面。

步骤3 在需要认证的域名所在行的操作列中，单击“前往认证”。

步骤4 弹出“认证域名”对话框，有两种域名认证方式，“上传证书认证”和“云上租户一键认证”。

方法一：选择“上传证书认证”，如[图1 上传证书失败](#)所示。

图 4-3 上传证书失败



1. 单击“下载认证文件”。
2. 将下载的认证文件上传到网站根目录，保证能成功访问链接“目标网址/hwwebscan_verify.html”。
3. 勾选“我已阅读并同意《华为云漏洞扫描服务免责声明》”。
4. 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”。

方法二：选择“云上租户一键认证”，如图2 云上租户一键认证所示。

图 4-4 云上租户一键认证



勾选“我已阅读并同意《华为云漏洞扫描服务免责声明》”，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 任务列表

5.1 创建扫描任务

该任务指导用户创建扫描任务。

前提条件

已获得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 > 任务列表”，进入“任务列表”界面。
- 步骤3** 单击“创建任务”，进入“创建任务”界面。

图 5-1 创建任务



- 步骤4** 请根据表1 扫描设置参数说明进行扫描设置，设置后如图2 扫描设置所示。

表 5-1 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。



参数	参数说明
接收通知	开启后，当扫描任务完成时用户会收到短信的完成提醒。 ●  : 关闭 ●  : 开启

图 5-2 扫描设置



步骤5 (可选) 用户可以根据需要展开“高级设置”，如图3 高级设置所示。参照表2 高级设置参数说明设置参数。

图 5-3 高级设置

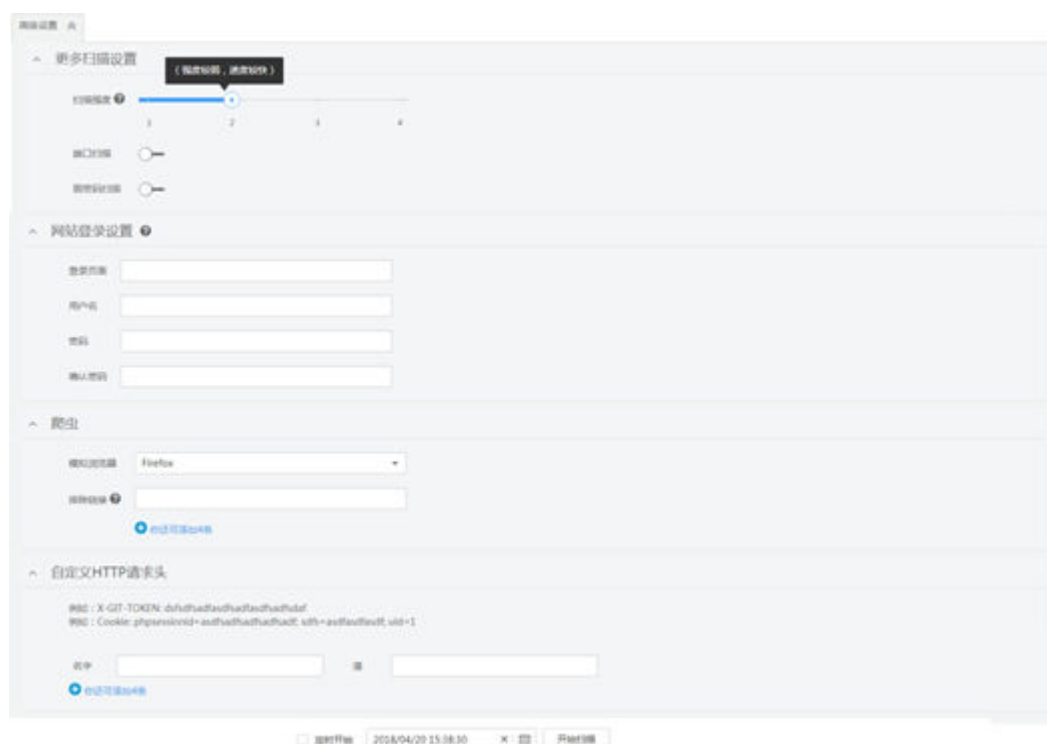


表 5-2 高级设置参数说明

参数	参数说明	设置
更多扫描设置		
扫描强度	扫描强度越高，检测能力越强，但是扫描耗时越久。	-
端口扫描	可以开启或关闭端口扫描。	 ：开启。
弱密码扫描	可以开启或关闭弱密码扫描。	 ：关闭。
网站登录设置		
说明 登录后才可以访问的页面，需要提供该信息才能进行扫描。		
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		
爬虫设置		
模拟浏览器	爬虫所使用的浏览器。	根据下拉框进行选择，目前支持 Firefox 和 Chrome。
排除链接	可以排除不需要进行扫描的页面。	最多可以添加 5 个链接，单击  可以添加多个链接，单击  可以删除添加的链接。
自定义 HTTP 请求头		
说明 对于有其他特殊访问要求的页面（例如需要输入验证码的页面），请填写 HTTP 请求头。 最多可以添加 5 个请求头，单击  可以添加多个 HTTP 请求头，单击  可以删除添加的请求头。		
名字	HTTP 请求头的名字。	示例： <i>Cookie</i>
值	HTTP 请求头的值。	示例： <i>phpsessionid=asdfsadfsadfsadfsadf;</i> <i>sdfs=asdfsadfsadfsadfsadf; uid=1</i>

步骤6 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。

- 定时扫描

勾选“定时开始”，设置好时间后，单击“定时开始”，系统会在用户设置的时间点启动该任务。

- 立即扫描

单击“开始扫描”，创建任务成功后直接跳转到“任务详情”页面。

 说明

如果服务器还有空闲，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

5.2 查看扫描详情

该任务指导用户查看扫描详情。

前提条件

- 已获取管理控制台的登录账号与密码。
- 已创建扫描任务。

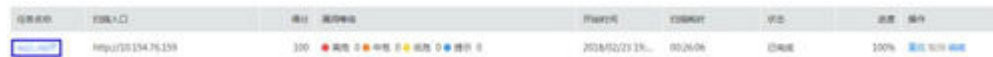
操作步骤

步骤1 登录管理控制台。

步骤2 选择“安全 > 漏洞扫描服务 > 任务列表”，进入“任务列表”界面。

步骤3 单击任务名称，如图1 任务名称所示。

图 5-4 任务名称



任务名称	扫描入口	统计	漏洞等级	开始时间	扫描耗时	状态	进度	操作
http://10.154.76.133		100	高危 0 中危 0 低危 0 漏洞 0	2018/02/23 13:...	00:26:06	已完成	100%	查看详情

步骤4 进入“任务详情”界面，可以查看相应任务的“扫描项总览”，如图2 扫描详情所示，各栏目说明如表1 详情总览说明所示。

 说明

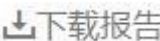
单击右上角的  可以下载任务报告，目前只支持 HTML 格式。

图 5-5 扫描详情



漏洞扫描服务 > 漏洞扫描服务 > 任务列表 > http://www.test.com

扫描地址: http://www.test.com

语言: zh-CN

漏洞等级: 0 高危 0 中危 0 低危 0 漏洞 0

开始时间: 2018/04/19 10:23:04 GMT+08:00

扫描耗时: 00:00:15

扫描结果: 包含高危漏洞 1 个，中危漏洞 0 个，低危漏洞 0 个，未发现漏洞 0 个。


任务高级设置详情

扫描项总览 漏洞列表 漏洞列表 站点结构

检测类型	检测项目	检测结果

点击下载报告

表 5-3 详情总览说明

栏目	说明	操作
扫描地址	从当前页面开始扫描。默认值是创建任务时填写的“目标网址”。	<ul style="list-style-type: none"> ● 单击目标网址后面的图标  可以查看网站的基本信息包括： <ul style="list-style-type: none"> - IP - 服务器 - 语言
任务信息	<p>显示目标任务的基本信息，包括：</p> <ul style="list-style-type: none"> ● 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。 ● 安全级别：根据扫描的结果分析网站的安全级别。如果无漏洞显示为安全，反之，有漏洞会按照漏洞的危险程度来显示中危、高危等。 ● 总数：漏洞总数及各级别的漏洞个数。 ● 开始时间：任务扫描的开始时间。 ● 扫描耗时：任务扫描耗时。 ● 扫描强度：创建扫描任务时选的对网站的扫描强度，一般扫描强度越深，扫描速度越慢。 ● 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。 	<ul style="list-style-type: none"> ● 单击“重新扫描”或“取消扫描”，可以重新扫描或取消扫描任务。 ● 单击“更多”，可以执行以下操作： <ul style="list-style-type: none"> - 查看高级设置详情 - 编辑扫描任务
扫描项总览	显示扫描任务的扫描项和扫描的类型以及每个扫描项的扫描结果。	<p>扫描结果：</p> <ul style="list-style-type: none"> ● 安全 ● 危险，单击“查看详情”。 ● 未进行域名认证，无法扫描，单击“立即进行域名认证”完成认证。

步骤5 “扫描项总览”显示扫描任务的扫描项和扫描的类型以及每个扫描项的扫描结果。扫描结果如果为安全且未认证可以单击“查看详情”了解详细情况。如果有危险（中危、高危等）请单击“查看详情”了解风险的内容。

图 5-6 扫描项总览

任务类型	任务名称	任务状态
Web 内容	网页木马	扫描中
	目录遍历	扫描中
	目录枚举	已完成
Web 网站	HTTP 响应	高危 24 高危漏洞 查看详情
	网站漏洞扫描	已完成
	服务器信息	高危 服务器信息认证, 无法获取数据 查看详情
	用户数据泄露	高危 服务器信息认证, 无法获取数据 查看详情
	敏感文件目录枚举	高危 服务器信息认证, 无法获取数据 查看详情
	文件完整性检查	高危 服务器信息认证, 无法获取数据 查看详情
网站安全漏洞	暴力破解	高危 服务器信息认证, 无法获取数据 查看详情
	反弹	高危 服务器信息认证, 无法获取数据 查看详情

步骤6 单击“漏洞列表”页签，进入“漏洞列表”的详情列表界面。

图 5-7 漏洞列表

漏洞ID	添加时间	标题	状态	类型	目标网址
a18752983e17b88f8a153e6c3e4429	2018/02/26 09:54:43 GMT+08:00	中	扫描	自我发现	http://20.93.194.177:8088/owa/images
4c9f91a9c1e40c8c1528f1a46a90183e	2018/02/26 09:54:42 GMT+08:00	中	扫描	自我发现	http://20.93.194.177:8088/owa/tao
e47c5886a978a107395329622547a1	2018/02/26 09:54:42 GMT+08:00	中	扫描	自我发现	http://20.93.194.177:8088/owa
73e13d17e1871933e9e8a8172a7c37	2018/02/26 09:53:52 GMT+08:00	中	扫描	弱口令爆破	http://20.93.194.177:8088/login.php
a18752983e17b88f8a153e6c3e4429	2018/02/26 09:54:43 GMT+08:00	中	扫描	自我发现	http://20.93.194.177:8088/owa/images

说明

- 显示目标任务最新发现的漏洞信息，单页最多显示 5 条，可以通过翻页进行查看。
- 单击“查看更多”，可以查看漏洞列表。
- 单击漏洞 ID 可以查看相应漏洞的“漏洞详情”。

步骤7 单击“端口列表”页签，进入“端口列表”的详情列表界面，显示目标网站的端口信息。

图 5-8 端口列表

端口	状态	协议	服务
22	关闭	TCP	NetBIOS Session Service1
23	打开	UDP	NetBIOS Session Service2
22	打开	TCP	NetBIOS Session Service2
22	打开	TCP	NetBIOS Session Service2
22	打开	TCP	NetBIOS Session Service2

步骤8 单击站点结构页签，进入“站点结构”的详情列表界面。

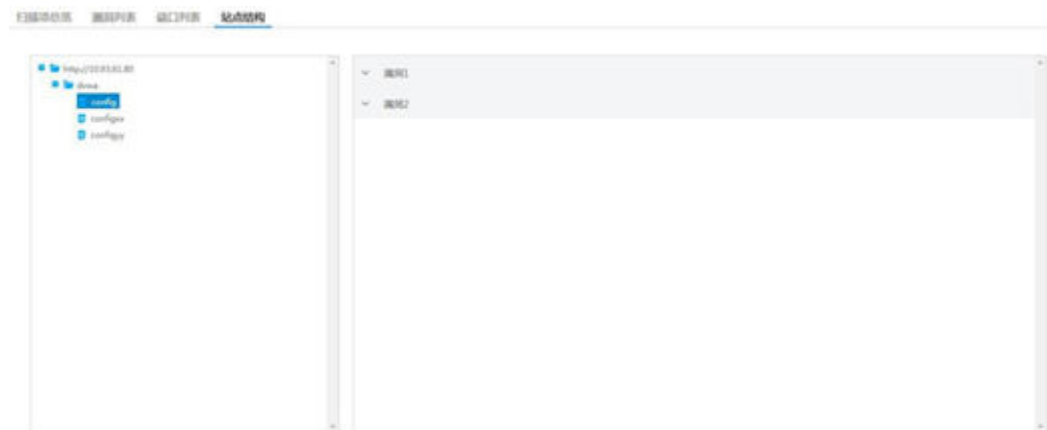
 说明

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 5-9 站点结构



----结束

6 总览

6.1 查看扫描概况

该任务指导用户通过“总览”查看扫描概况，主要展示漏洞概览、最新漏洞新闻、漏洞类型、漏洞等级、漏洞列表、最新扫描情况和产品资讯。

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 > 总览”，进入“总览”界面。

步骤3 扫描概况如[图1 总览](#)所示，各栏目说明如[表1 总览说明](#)所示。

说明

通过左上方的域名下拉框可以选择已认证通过的域名，查看 VSS 为所选域名发现的漏洞的统计信息。

图 6-1 总览

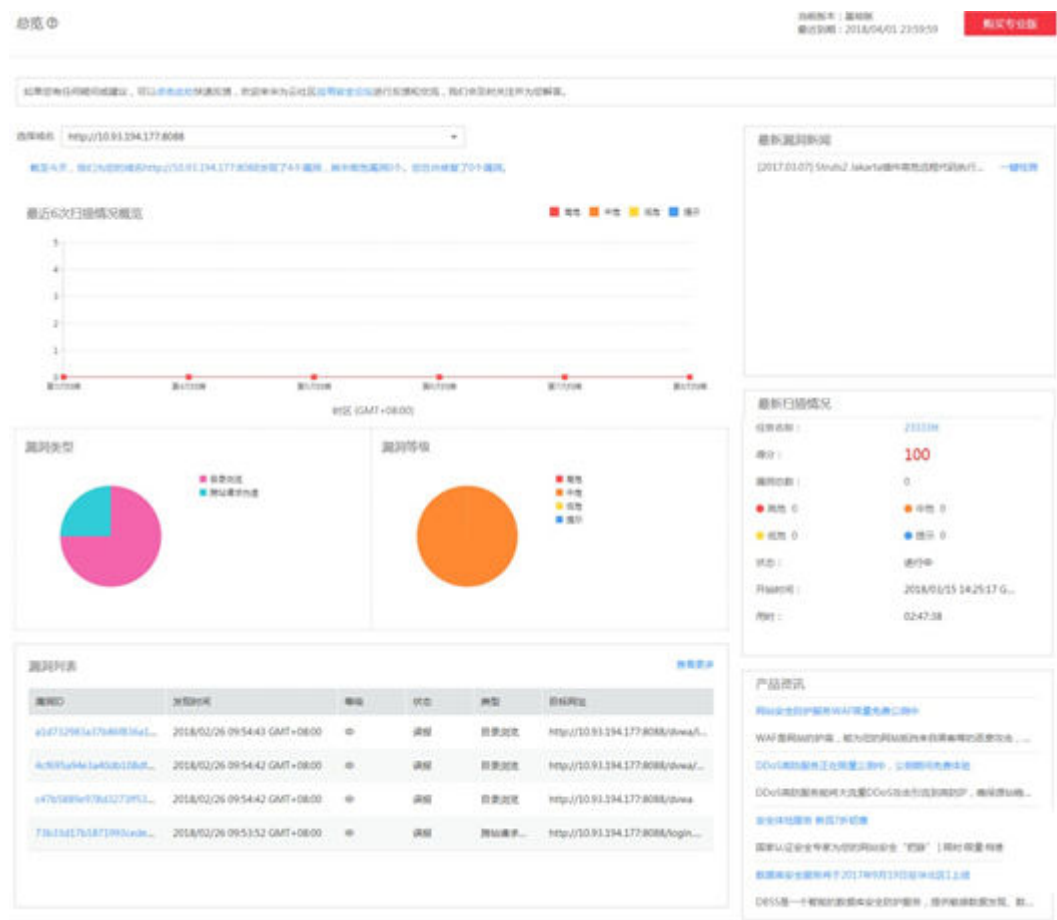


表 6-1 总览说明

栏目	说明	操作
最近 6 次扫描情况概览	显示VSS 为用户所选域名发现的各级别的漏洞个数随扫描时间（最近 6 次）的曲线分布图。	当不需要展示某种漏洞等级的数据时，单击图形右侧对应的图例，可隐藏相应类型的数据统计。 单击 高危，可以隐藏高危漏洞的统计。
漏洞类型	显示VSS 为用户所选域名发现的漏洞所属类型分布图。	当不需要展示某种漏洞类型的数据时，单击图形右侧对应的图例，可隐藏相应类型的数据统计。 例如： 单击 SQL注入，可以隐藏 SQL 注入漏洞的统计。
漏洞列表	显示VSS 为所选域名发现的漏洞信息列表，包括漏洞编号、发现时间、漏洞等级、漏洞状态、类型和URL。	<ul style="list-style-type: none"> 单击漏洞 ID 可以查看相应漏洞的“漏洞详情”，具体请参见查看漏洞详情。 单击“查看更多”可以跳转到“漏洞列表”界面。

栏目	说明	操作
最新漏洞新闻	显示VSS 需要紧急处理的漏洞信息。	单击“一键检测”进入“一键检测最新紧急漏洞风险”页面查看详情。
最新扫描情况	显示最近一次扫描任务的信息，包括任务名称、得分、各等级的漏洞数量、状态、开始时间和用时。	单击任务名称可以查看相应任务的“任务详情”，具体请参见 查看扫描详情 。
产品资讯	显示VSS 或者其他相关产品信息。	-

---结束

6.2 漏洞列表

6.2.1 查看漏洞列表

该任务指导用户查看扫描出的漏洞列表。

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 > 总览”，进入“总览”界面。

步骤3 在“漏洞列表”区域右侧，单击“查看更多”，进入“漏洞列表”界面，如[图1 漏洞列表](#)所示，相关参数请参见[表1 漏洞列表参数说明](#)。

说明

用户可以通过筛选“所有状态”下拉框，或展开高级搜索，选择“发现时间”、筛选“所有漏洞类型”下拉框、选择“漏洞级别”，单击“查询”，过滤需要查看的漏洞。单击“重置”可以清除高级搜索条件。

图 6-2 漏洞列表



漏洞ID	发现时间	等级	状态	类型	目标网址
a1d732983a37b86f836a1...	2018/02/26 09:54:43 GMT+08:00	中	已忽略	目录浏览	http://10.93.194.177:8088/dvwa/...
4c695a94e3a40cb108df...	2018/02/26 09:54:42 GMT+08:00	中	已忽略	目录浏览	http://10.93.194.177:8088/dvwa/...
c47b5889e978d3273ff53...	2018/02/26 09:54:42 GMT+08:00	中	已忽略	目录浏览	http://10.93.194.177:8088/dvwa
73b33d17b1871993cede...	2018/02/26 09:53:52 GMT+08:00	中	已忽略	跨站请求...	http://10.93.194.177:8088/login...

表 6-2 漏洞列表参数说明

参数名称	说明
漏洞 ID	漏洞编号。单击漏洞 ID 可以查看相应漏洞的“漏洞详情”。
目标网址	漏洞所在页面。
发现时间	发现漏洞的时间。
等级	漏洞的等级，包括： <ul style="list-style-type: none"> ● 高：高危 ● 中：中危 ● 低：低危 ● 提示
类型	漏洞类型，包括SQL 注入、反射型XSS、跨站请求伪造等。
状态	漏洞状态，包括： <ul style="list-style-type: none"> ● 未修复 ● 已修复 ● 已忽略

---结束

6.2.2 查看漏洞详情

该任务指导用户查看目标漏洞的漏洞详情。

前提条件

- 已获取管理控制台的登录账号与密码。
- 已扫描出漏洞。

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 > 总览”，进入“总览”界面。

步骤3 在“漏洞列表”区域右侧，单击“查看更多”，进入“漏洞列表”界面。

步骤4 单击漏洞 ID，如[图1 漏洞ID](#)所示。

图 6-3 漏洞 ID

漏洞ID	目标网址	漏洞描述	发现时间	等级	类型	状态	操作
1147202020202020	http://10.91.134.177:8086/okwa/images	wpt_allen	2018/02/06 09:54:43 GMT+08:00	中	跨站请求	已忽略	详情 删除
1147202020202020	http://10.91.134.177:8086/okwa/oa	wpt_allen	2018/02/06 09:54:42 GMT+08:00	中	跨站请求	已忽略	详情 删除

步骤5 进入“漏洞详情”界面，可以查看相应漏洞的详细信息，如[图2 漏洞详情](#)所示，各栏目说明如[表1 漏洞详情说明](#)所示。

图 6-4 漏洞详情



表 6-3 漏洞详情说明

栏目	说明	操作
漏洞详情	显示目标漏洞的基本信息，包括漏洞编号、漏洞等级、漏洞状态、发现时间、漏洞类型、所属域名、URL、漏洞简介。	单击“标记为忽略”可以将该漏洞忽略。 说明 当一个漏洞被标记为“忽略”之后，则不可更改状态，系统不再认为该漏洞有风险，单击“恢复”可以取消忽略。
修复建议	相应漏洞的修复建议。	-
命中详情	是否为漏洞的判断依据。	-
请求详情	VSS 模拟黑客对目标网站进行探测和攻击尝试的请求内容。	-
响应详情	目标网站对 VSS 模拟请求的响应内容。	-

---结束

6.2.3 标记为忽略

该任务指导用户将那些经分析确认没有安全风险的漏洞标记为“忽略”。

说明

当一个漏洞被标记为“忽略”之后，则不可更改状态，系统不再认为该漏洞有风险，单击“恢复”可以取消忽略。

前提条件

- 已获取管理控制台的登录账号与密码。
- 已扫描出漏洞。

操作步骤

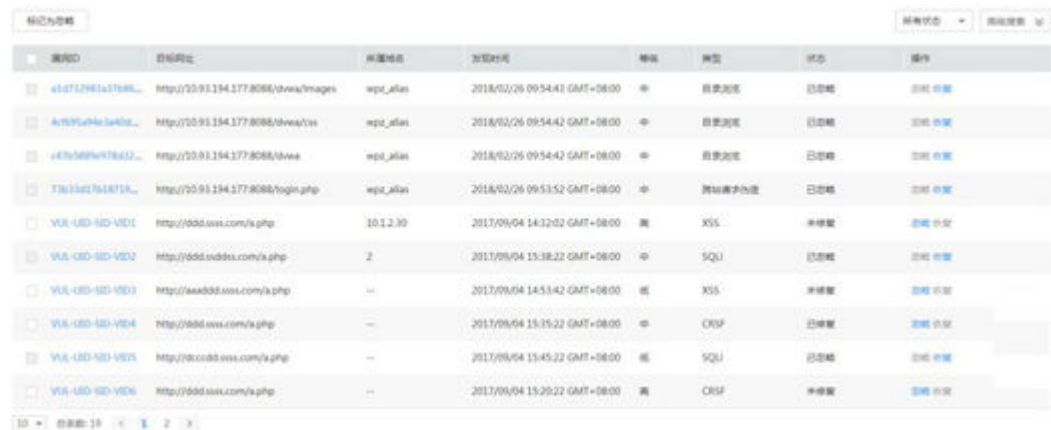
步骤1 登录管理控制台。

步骤2 选择“安全 > 漏洞扫描服务 > 总览”，进入“总览”界面。

步骤3 在“漏洞列表”区域右侧，单击“查看更多”，进入“漏洞列表”界面。

步骤4 选中需要忽略的漏洞，单击“标记为忽略”，如图1 标记为忽略所示。

图 6-5 标记为忽略



ID	漏洞ID	目标网址	来源地址	发现时间	等级	类型	状态	操作
	41471791a3798...	http://20.93.194.177.8088/static/images	wpt_allan	2018/02/26 09:54:41 GMT+08:00	中	目录遍历	已忽略	忽略 详情
	4c9b9fa9e5a46a...	http://20.93.194.177.8088/static/css	wpt_allan	2018/02/26 09:54:42 GMT+08:00	中	目录遍历	已忽略	忽略 详情
	4c9b9fa9e5a46a...	http://20.93.194.177.8088/static/js	wpt_allan	2018/02/26 09:54:42 GMT+08:00	中	目录遍历	已忽略	忽略 详情
	73a134d7618718...	http://20.93.194.177.8088/login.php	wpt_allan	2018/02/26 09:53:52 GMT+08:00	中	跨站脚本攻击	已忽略	忽略 详情
	VUL-182-182-VIE1	http://666.xxx.com/a.php	10.1.2.30	2017/09/04 14:32:02 GMT+08:00	高	XSS	未修复	忽略 详情
	VUL-182-182-VIE2	http://666.xxx.com/a.php	2	2017/09/04 15:38:22 GMT+08:00	中	SQLI	已忽略	忽略 详情
	VUL-182-182-VIE3	http://aaabbb.xxx.com/a.php	--	2017/09/04 14:53:42 GMT+08:00	低	XSS	未修复	忽略 详情
	VUL-182-182-VIE4	http://666.xxx.com/a.php	--	2017/09/04 15:35:22 GMT+08:00	中	CRF	已忽略	忽略 详情
	VUL-182-182-VIE5	http://666.xxx.com/a.php	--	2017/09/04 15:45:22 GMT+08:00	低	SQLI	已忽略	忽略 详情
	VUL-182-182-VIE6	http://666.xxx.com/a.php	--	2017/09/04 15:20:22 GMT+08:00	高	CRF	未修复	忽略 详情

说明

- 用户也可以在需要标记为忽略的漏洞所在行的“操作”列，单击“忽略”，标记单个漏洞。
- 用户还可以在“漏洞详情”界面，单击“忽略”，标记单个漏洞。

步骤5 在弹出的“忽略风险项”对话框中，单击“确定”，将所选漏洞标记为“忽略”。

----结束

A 修订记录

发布日期	修改说明
2019-07-12	第三次正式发布。 <ul style="list-style-type: none">● 增加“开通VSS章节”。● 增加常见问题“价格体系”。● 增加常见问题“续费”。● 增加常见问题“退订”。
2019-07-08	第二次正式发布。 内容优化。
2018-05-10	第一次正式发布。