

漏洞扫描服务

操作指南

产品文档



腾讯云

【 版权声明 】

©2013-2021 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【 商标声明 】



及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【 服务声明 】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【 联系我们 】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100。

文档目录

操作指南

添加白名单 IP

添加资产

模拟登录

操作指南

添加白名单 IP

最近更新时间：2021-04-23 10:55:59

本文档将为您详细介绍如何将腾讯云漏洞扫描服务的监测 IP 加入到白名单。

操作场景

漏洞扫描服务通过公网进行资产发现和风险监测时会使用模拟黑客入侵攻击的方式。如果您的服务器有安全防护或监控部署（例如 WAF、SOC），建议您将腾讯云漏洞扫描服务的监测 IP 加入到白名单中，开启扫描访问权限，保证监控服务正常运行，漏洞扫描服务扫描节点 IP 为：

129.211.162.110
129.211.162.87
129.211.163.253
129.211.164.19
129.211.166.123
129.211.167.182
129.211.167.200
129.211.167.70
129.211.162.158
129.211.162.23
129.211.166.134
129.211.167.108
129.211.167.181
129.211.166.142
129.211.166.163
129.211.167.128
129.211.167.166

若您的网站需登录才可以访问，则需要先解除安全策略（即确保所有 IP 都能访问），待您的 cookie 有效性验证通过后再恢复限制。

操作步骤

方式1：通过 IP 查询添加白名单

1. 登录 [Web 应用防火墙控制台](#)，在左侧导航中，选择【IP 管理】>【IP 查询】，进入 IP 查询页面。

2. 在 IP 查询页面，输入需要查询的 IP 地址，单击【查询】，将展示查询结果。

查询结果

IP	193.170.255.100	拦截
域名	-	
拦截开始时间:	2020-06-16 15:21:35	
拦截结束时间:	2020-06-30 23:59:59	
类别	黑名单	
触发策略名称	whitelp	

[加入黑白名单](#)

3. 单击【加入黑白名单】，进入“添加黑白 IP”页面，可手动添加白名单。类别选择“白名单”，IP 地址填写需要添加到白名单的地址，选择白名单有效期的截止时间，设置完成后，单击【添加】，即完成白名单添加。

添加黑白IP

类别 黑名单 白名单

IP地址

截止时间 *

备注

方式2：直接添加 IP 白名单

登录 [Web 应用防火墙控制台](#)，在左侧导航中，选择【IP 管理】>【IP 黑白名单】，进入 IP 黑白名单页面。

方式1：手动添加白名单。

- i. 在 IP 黑白名单页面，单击【添加黑白名单】，将弹出“添加黑白IP”窗口。
- ii. 在“添加黑白IP”窗口中，类别“白名单”类别，将漏洞扫描服务扫描节点 IP 复制到 IP 地址的输入框内，选择白名单有效期的截止时间，设置完成后，单击【添加】，即完成白名单添加。

说明：

最多支持输入100个 IP 地址，多个 IP 地址以换行分隔。

添加黑白IP

类别



黑名单



白名单

IP地址

```
193.112.70.224
193.112.71.109
193.112.70.227
193.112.71.33
193.112.72.165
```

截止时间 *

2019-12-05



23:59:59

备注

非必填项，200个字符以内

添加

取消

方式2：批量导入白名单。

- i. 在 IP 黑白名单页面，单击【导入数据】，将弹出“导入 IP 名单”窗口。
- ii. 在“导入 IP 名单”窗口中，单击【导入】，选择导入白名单文件，上传完成后，单击【确认导入】即可。

说明：

- 导入文件格式：仅支持.xlsx、.xls。
- 数量：目前只支持单个文件上传。
- 内容：必须包含类别，IP 地址，截止时间三列，具体可参考导出数据 excel 格式。
- 截止时间，必须在2033/12/30 23:59:59之前，格式 YYYY/MM/DD HH:MM:SS。

导入IP名单



导入

点击按钮，选择文件。

说明：

- 1.格式，仅支持.xlsx，.xls。
- 2.数量，目前只支持单个文件上传。
- 3.内容，必须包含类别，IP地址，截止时间三列；具体可参考导出数据excel格式。
- 4.截止时间，必须在2033/12/30 23:59:59之前，格式YYYY/MM/DD HH:MM:SS。

确认导入

重置

方式3：将已封堵 IP 添加白名单

1. 登录 [Web 应用防火墙控制台](#)，在左侧导航中，选择【IP 管理】>【IP 封堵状态】，进入 IP 封堵状态。
2. 在 IP 封堵状态页面，输入相关信息，单击【查询】，可以查询漏洞扫描服务的相关 IP 信息，即可对已封堵 IP 进行加白操作。

类型： ▼

记录创建时间：最近5分钟 最近10分钟 最近30分钟 2020-06-19 16:05:55 至 2020-06-19 23:59:59 📅

有效截止时间：2020-06-19 16:10:55 至 2020-06-27 16:10:55 📅

触发策略： ⓘ

IP地址：

查询

添加资产

最近更新时间：2020-09-18 18:48:06

本文档将指导您如何在漏洞扫描服务控制台添加资产。

操作场景

您可以在资产管理页面添加资产，添加完成后即可对资产进行漏洞扫描。目前支持添加所有使用域名、IP 或公众号访问的网站，支持添加主机，支持添加 API。

操作步骤

1. 登录 [漏洞扫描服务控制台](#)，在左侧导航中，单击【资产管理】，进入资产管理页面。
2. 在资产管理页面，单击【添加资产】，将弹出“使用须知”弹窗。
3. 在“使用须知”弹窗中，阅读使用须知，并勾选“我已阅读并了解产品相关服务说明及条件约束”，单击【确定】，进入添加资产页面。

使用须知

- 1、您使用漏洞扫描服务进行扫描的业务须为正常的商业、科研等符合国家法律规定的业务，不得用于从事任何非法业务。
- 2、您使用漏洞扫描服务进行扫描的业务必须为自有业务，不得对其他任何第三方业务进行扫描；若违反该约定的，腾讯云有权立即终止您的使用，且造成的腾讯云及任何第三方的全部损失均由您承担。
- 3、您承诺不利用漏洞扫描服务系统进行任何破坏或试图破坏网络安全的行为（包括但不限于钓鱼、黑客、网络诈骗、散播病毒木马、ARP欺骗、DDoS等）。
- 4、您应仔细阅读漏洞扫描服务的指引和说明，自行判断漏洞扫描服务与您的服务的适配性，并依照相关操作指引进行操作。由您手动设置的部分及其产生的结果由您自行负责，请您自行把握风险并谨慎操作。

我已阅读并了解产品相关服务说明及条件约束。

下次不再提醒

确定

4. 在添加资产页面，选择任意类型，并输入相应信息，输入完成后，单击【添加】即可。

注意：

添加网站时，可输入多个地址，每个地址以换行分隔。

资产类型 网站 主机 API

网站类型 * 域名 IP 公众号

地址 *

请每行输入一个地址，例如
https://console.cloud.tencent.com:8080
http://dwwa.webscantest.cn:443

添加

取消

模拟登录

最近更新时间：2021-01-08 16:19:59

操作场景

如果您的网站部分或全部页面、功能需要登录才能访问，建议设置 Cookie 以模拟登录网站进行全面扫描，以获得全面的漏洞扫描结果。目前支持通过设置登录成功后的 Cookie 方式模拟登录网站进行扫描，并且后台会定时携带您填写的 Cookie 访问网站以保证 Cookie 不失效。

操作步骤

模拟登录网站设置

1. 登录 [漏洞扫描服务控制台](#)，在左侧导航中，单击【资产管理】，进入资产管理页面。
2. 在资产管理页面，单击【网站】，找到需要模拟登录的资产。
3. 在需要模拟登录的资产所在行，找到“模拟登录”列，单击【设置】，弹出“模拟登录”窗口。

资产	类型	添加时间	认证状态	模拟登录 
http://1.1.1.1	IP	2020-06-16 15:43:28	已认证	未设置 设置

4. 在“模拟登录”窗口中，输入正确 Cookie 值（请参见 [Cookie 值获取方法](#)），单击【保存】。

模拟登录



资产

Cookie值

例如：\userid=123456789; sessionid=abcdfg123456

模拟登录可能会影响您的业务系统，请谨慎使用

[如何获取cookie值](#)

保存

取消

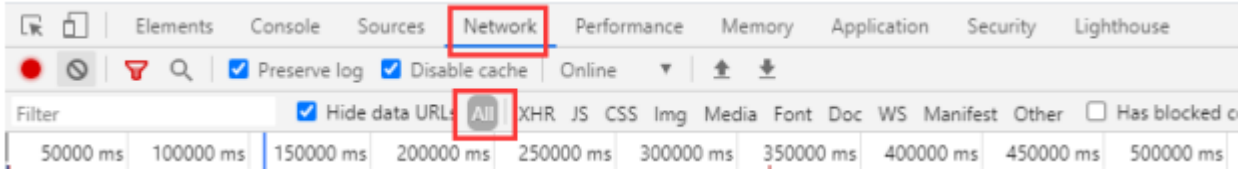
5. 模拟登录网站设置完成。

Cookie 值获取方法

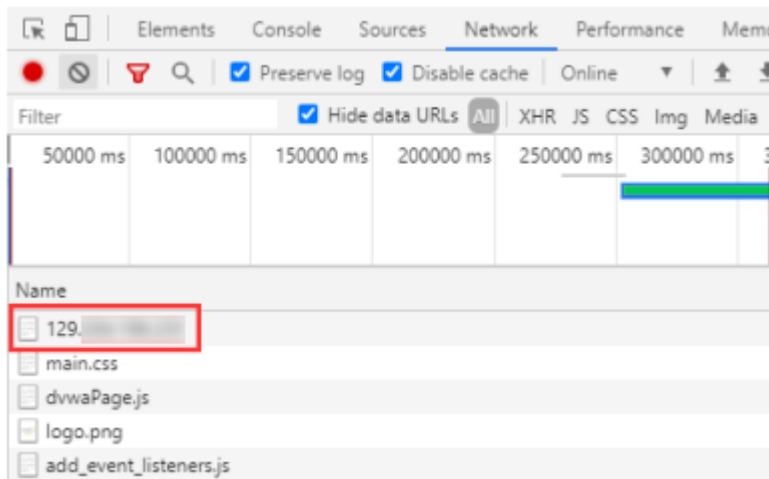
1. 请先使用 Chrome 浏览器成功登录您网站，访问一个需要登录才能继续访问的页面，使用 F12 或在页面右键选择“检查”。

查看网页源代码(V) Ctrl+U
 查看框架的源代码(V)
 重新加载框架(F)
检查(N) Ctrl+Shift+I

2. 在出现的开发者工具中选择【 Network 】>【 All 】，并刷新页面。



3. 单击排在第一的网络请求。



4. 在“Headers”中找到“Cookie”这一项，拷贝该 Cookie 值即可。

