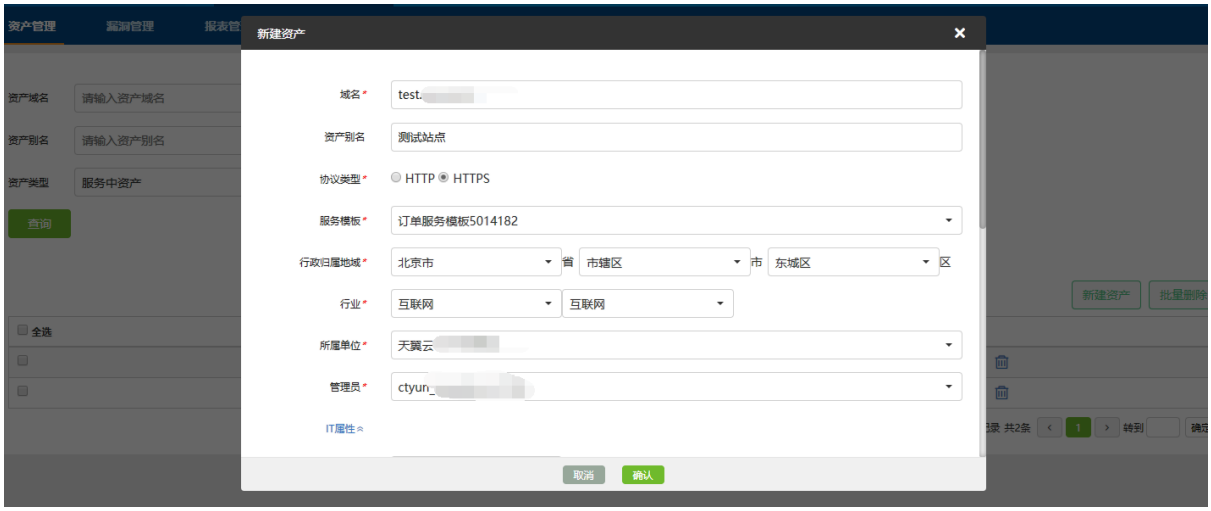
天翼云 • 网站安全检测服务

用户使用指南

中国电信股份有限公司云计算分公司

目 录



1 产品介绍

1.1 产品定义

网站安全检测服务是托管式 SaaS 安全服务，为客户提供网站漏洞扫描及漏洞验证、网页挂马检测、网页篡改检测、网页敏感内容检测以及网站可用性检测、域名解析检测服务。7x24 小时远程安全检测，帮助客户了解网站安全状况。

网站安全检测服务是一款托管式服务。您无需安装任何硬件或软件，无需改变目前的网络部署状况，无需专门的人员进行安全设备维护及分析日志，用户购买后即可享受 7×24 小时的远程网站安全检测服务。一旦发现您的网站存在风险状况，安全专家团队会第一时间通知您，并提供专业的安全解决建议。除此之外，经验丰富的安全专家团队会定期为您出具周期性的综合评估报告，让您整体掌握网站的风险状况及安全趋势。

凭借专业化的服务产品来实时检测和周期度量网站的风险隐患，您可以轻松评估您网站的安全状态，跟踪改进情况，能够将网站管理人员从繁重的日常安全维护工作中解放出来，降低投入和管理成本，获得最专业、最有效、最便捷的服务，同时还遵从了政府和行业的信息安全法规要求。

1.2 术语解释

SaaS：即安全即服务的简称。它是一种通过 Internet 提供安全能力的模式，厂商将应用软件统一部署在自己的服务器或云平台上，客户可以根据自己实际需求，通过互联网向厂商定购所需的应用软件服务，按定购的服务多少和时间长短向厂商支付费用，并通过互联网获得厂商提供的服务。

1.3 产品功能

- 网站安全检测服务——一站式全托管 7×24 小时网站安全远程检测服务。
- 完整性检测：包括网页挂马检测、网页篡改检测、敏感内容检测服务；
- 脆弱性检测：包括网站漏洞扫描和安全专家漏洞验证服务；
- 可用性检测：包括网站平稳度检测、域名解析检测服务；

1.4 产品优势

- **应用快、检测快、响应快：**7*24 小时全天候服务，按需购买，即买即用，无需安装部署。平台每 15 分钟检测一次，高密度发现网站异常情况，安全专家 30 分钟内分析告警，及时响应告警事件。
- **定位问题快：**用户各单位的风险及事件以组织架构形态做可视化呈现，让用户对于所辖单位暴露的问题一目了然。同时用户在排查问题时可以得到更多的诊断信息的帮助，例如 “通断时长、链路、检测点，协议等”
- **漏洞、事件覆盖广：**支持扫描网站系统漏洞，支持扫描 WASC 25 种 Web 应用漏洞，全面覆盖 OWASP Top 10 Web 应用风险。支持检测挂马、篡改、敏感内容、平稳度、域名解析、黑链等安全事件的检测，并可以在用户门户上做可视化呈现。
- **检测点分布广：**支持多点检测，覆盖全国多省、三大运营商线路，覆盖部分海外城市。
- **免物流、免安装、免部署、免维护：**直接远程交付服务，无需走物流发货流程，纯 SaaS 服务，无需安装任何软硬件，成本低，无需改变网络结构，无需占用机房或办公空间，无需处理软硬件故障、升级等问题，完全托管，无需亲自运维。
- **精准验证高中危漏洞：**能够针对所有扫描出的高中危漏洞提供专家级漏洞验证。
- **精准贴合用户业务需求：**能够通过自定义可用性检测级别，更加贴合用户业务场景。
- **精准贴合用户管理规范：**能够通过分级告警的方式，更加贴合用户实际管理规范。

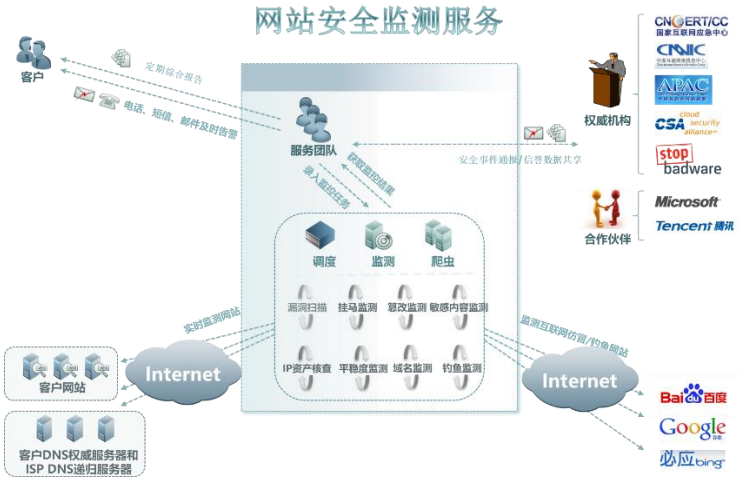
1.5 应用场景

响应合规性要求

满足等级保护检测方面要求，实时监控网站的安全状态、安全漏洞和安全事件。协助客户及时发现，修复网站存在的安全风险和问题，满足行业监管的相关考核、检查指标。

漏洞、事件的生命周期闭环管理

网站安全检测服务可有效地帮助用户进行漏洞生命周期的管理。服务从漏洞扫描、人工验证、漏洞状态追踪等方面，敏锐的洞悉用户站点的安全风险变化，并针对安全风险点给出合理的修补建议，以及漏洞修复后的复验工作。本服务并非只是进行简单的漏洞扫描工作，也是协助用户管控安全风险的有力工具。



网站高效运维

通过专业的远程托管式安全服务，按需付费，经济实惠，大大节省了用户在安全软件或设备方面的投入和维护成本，有效减少安全人员投入，节省人力成本和管理费用。能够将客户从繁重的日常安全维护工作中解放出来，提高工作效率，将精力集中在核心业务上。

重大时期保障

为政府、国企等客户提供重大时期的应急保障，7x24 小时监控网站可用性和网站内容，并提前进行脆弱性检测，保证网站不带病上岗。

政企类网站

避免页面被恶意篡改后对政府或企业形象造成不良影响。对于被挂马的网站，可及时通知客户清除挂马内容，避免网站被进一步恶意利用。

金融类网站

及时发现业务网站业务不可用的情况，避免由此造成的损失。

2 购买指南

2.1规格

网站安全检测服务分为基础版和高级版，具体功能如下。

规格	功能
基础版	对 WEB 以及系统漏洞进行扫描检测； 对各类 WEB 安全事件进行检测，包括挂马、黑链、敏感内容等； 定期提供检测报告；
高级版	对可用性提供多线路检测； 对域名劫持进行检测； 对 WEB 以及系统漏洞进行扫描检测； 漏洞跟踪验证服务； 对各类 WEB 安全事件进行检测：包括挂马、黑链、敏感内容等； 定期提供检测报告；

收费标准：根据版本、监测主域名数量、订购周期进行收费。

产品规格	标准价格（元/月）	
	基础版	高级版
10 域名套餐包	6000	10000
30 域名套餐包	16000	27000
50 域名套餐包	24000	40000
单独购买/域名	650	1100

备注：针对一次性包年付费服务，1、2、3 年包年标准价格按照 85 折计算。

3 操作指南

3.1 安全态势图

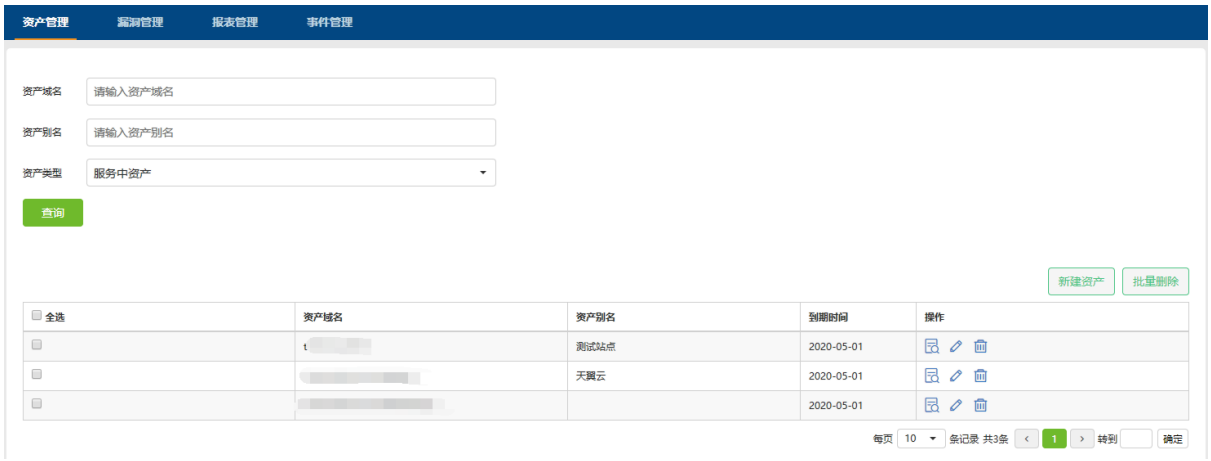
3.1.1 首页

选择菜单首页，进入首页，可以按照地理位置维度查看漏洞分布图、漏洞统计信息、安全事件统计信息和不同维度的 TOP 风险统计信息。

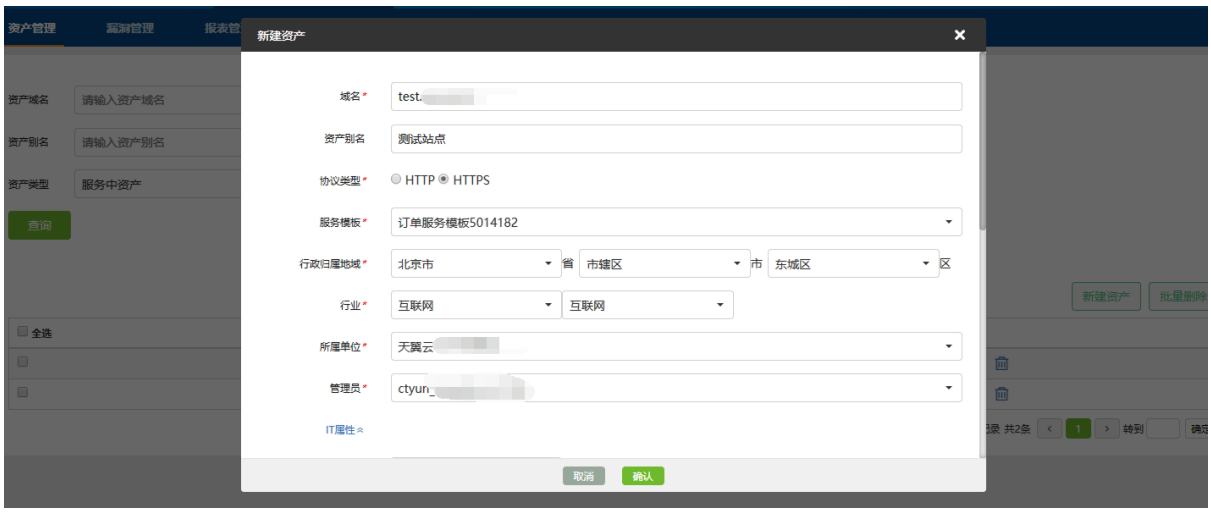
3.2资产管理

3.2.1 资产录入

进入“资产管理”页签，点击“新建资产”



输入站点信息，并勾选“IT 属性”中的免责声明，点击确认即可将站点添加至检测服务。



3.2.2 资产展示

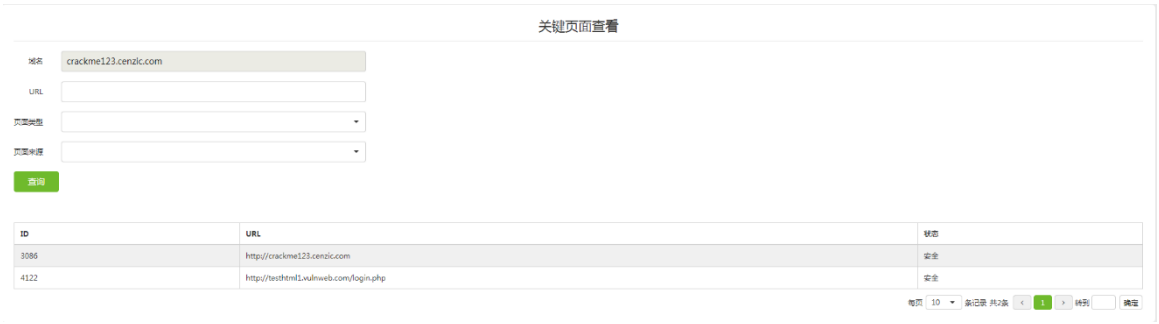
资产是客户网络环境中有价值的实体、是安全业务的管理对象。网站资产即网络中的一个站点，以域名或 URL 来标识。选择菜单资产管理，进入如下图所示页面：

3.2.3 资产查询

对于资产，可以按照资产域名、资产别名、资产类型进行搜索，如输入资产域名，点击“查询”，就可以搜索到该资产：

3.2.4 关键页面查看

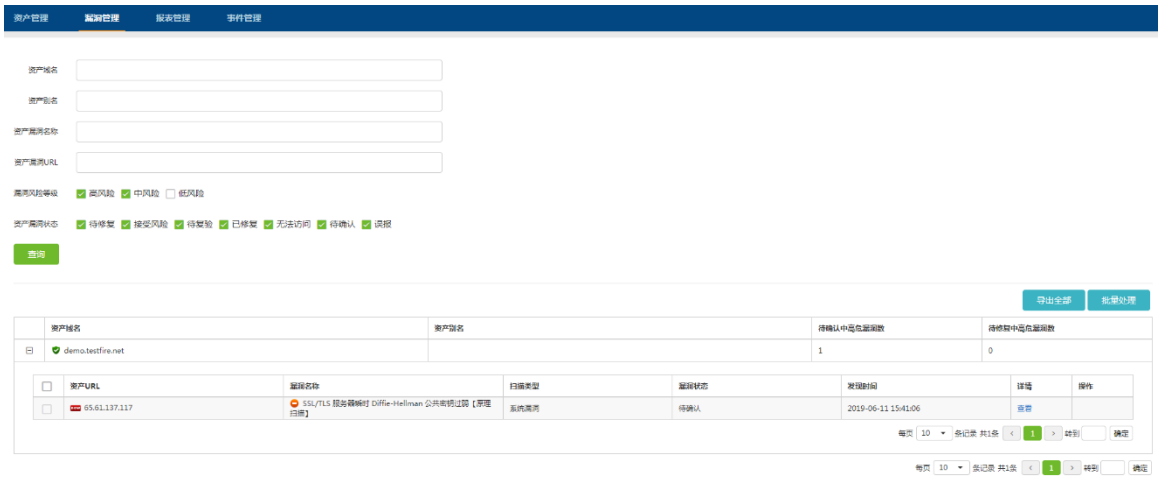
点击操作栏的 可以查看资产的关键页面，也可以按域名、URL、页面类型、页面来源查询：



3.3漏洞管理

3.3.1 漏洞展示

选择菜单漏洞管理，进入如下图所示页面，点击漏洞前面的“+”号，会展开漏洞的具体情况：



3.3.2 漏洞详情查看

对于具体漏洞，可以点击详情中的“查看”按钮进行查看该漏洞的相关信息。

3.3.3 漏洞处置

对于具体漏洞，可以处置状态

，点击处置：

3.3.4 导出漏洞

点击漏洞列表右上方的

可以导出漏洞

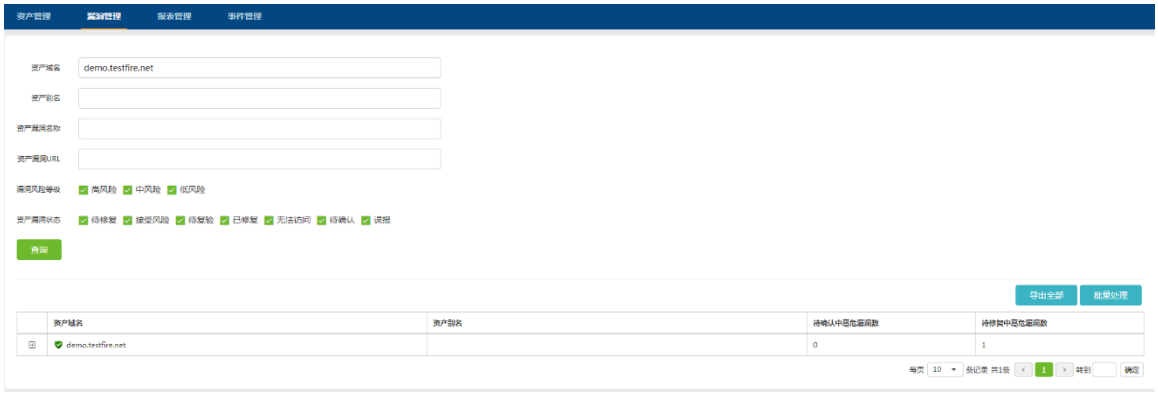
3.3.5 批量处理

点击漏洞列表右上方的 批量处理 可以批量处置漏洞

点击漏洞列表右上方的 批量处理 可以处理漏洞状态

3.3.6 漏洞查询

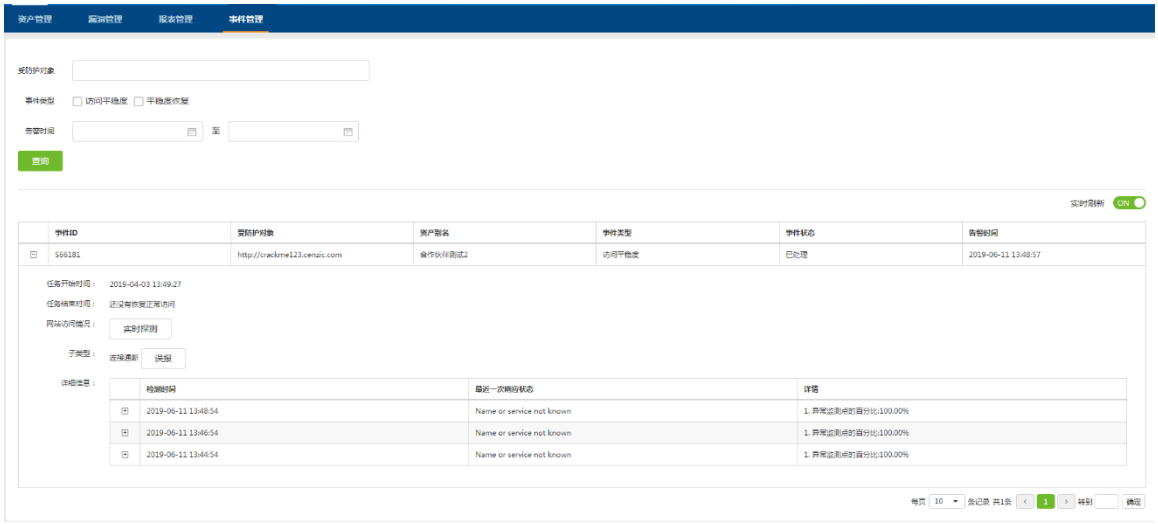
对于漏洞，可以按照资产域名、资产别名、资产漏洞名称、资产漏洞 URL、漏洞风险等级、资产漏洞状态进行搜索，如：



3.4事件管理

3.4.1 事件展示

选择菜单事件管理，进入如下图所示页面：



如果勾选了“实时刷新”，则该页签的事件量是实时刷新的。

点击事件前面的“+”号，会展开响应安全事件的详情页面，如上图所示。

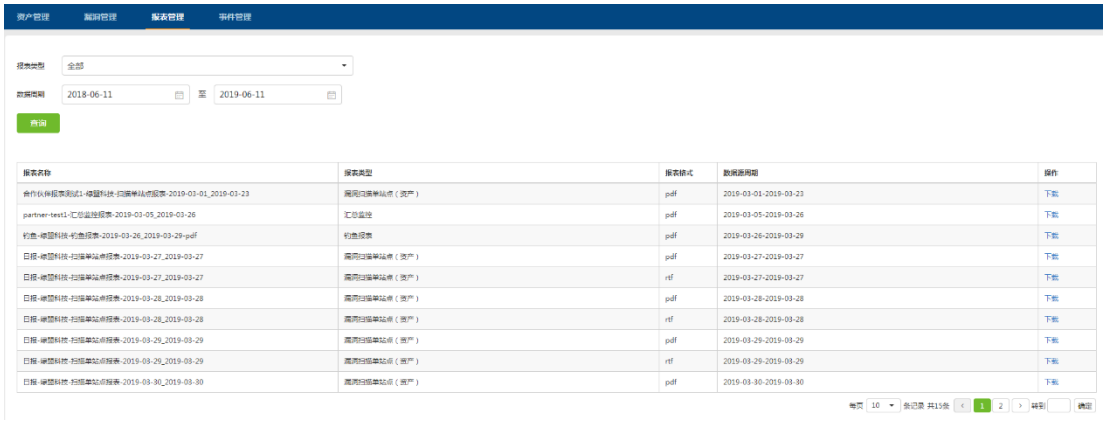
3.4.2 事件查询

对于事件，可以按照受防护对象、事件类型、告警时间进行搜索，如输入受防护对象，点击“查询”，就可以搜索到该对象的事件：

3.5报表管理

3.5.1 报表展示

选择菜单事件管理，进入如下图所示页面：



3.5.2 报表查询

对于报表，可以按照报表类型、数据周期进行搜索，如选择“汇总监控”，点击“查询”，就可以搜索到对应的报表：

4 常见问题

Q:当前可提供几种服务规格，收费方式是怎样规定的？

A：可提供 2 种服务规格，分别为基础版和高级版；收费方式为按照检测的站点数进行计费，服务周期为一年。具体价格详见文档 1.3 章节。

Q:如开通使用该服务，用户需提供自身网站的哪些信息？

A:用户需注册“天翼云”网站官方账号并实名认证，然后在服务购买时提交需要检测网站的域名、源站 IP、技术联系人等信息。

Q:是否可以检测图片或视频篡改？

A:主要是支持对网页 DOM 结构及文本内容变化的检测，暂不支持对图片、音频、视频的变更检测。

Q:漏洞扫描是否会对网站造成危害？

A:会对网站产生一定的探测压力，但不会对您的网站进行数据删除等破坏行为。

Q:网站安全检测服务报告发送频率？

A:页面安全类服务每周提供报告，扫描服务每月提供报告。

Q:扫描报表中的漏洞是否真实存在？

A:如购买了漏洞验证服务，报告中的高中危漏洞全部为真实存在。

Q:是否可以协助进行漏洞修复？

A:扫描报表中会提供漏洞的修复建议，但不提供远程或上门进行漏洞修复。

Q:使用该服务时用户网站需如何进行设置?

A:由于云端需要对被检测网站发起扫描、页面爬取以及平稳度检测，如果网站服务器所在网络部署了安全防护设备或者主机防火墙等软硬件，需要对云端的服务 IP（详见附录：网站安全检测服务出口 IP 列表）进行白名单处理，以免正常的服务内容因为访问阻断而无法提供。

5 附录：网站安全检测服务出口 IP 列表

网站安全检测服务在检测过程中，有可能被 WAF、入侵检测等安全设备判断为攻击行为而拦截，可能会**影响检测效果，导致检测失败**。请您在防护设备上将以下相关 IP 加入白名单或配置必要的放行策略，以确保检测服务正常运行。

网站安全检测各项服务使用出口 IP 如下表所示，如果您对下列 IP 的访问行为有疑问，请随时与我们联系。

服务	IP
敏感内容检测	221.122.179.200 221.122.66.200
网站挂马检测	
DNS 检测	
黑链检测	
篡改检测	
漏洞扫描	221.122.70.1-7 122.14.62.68 124.206.180.130 101.204.128.115 110.191.179.168