

# AppScan

---

## 入门

---

安全是为了保护您的宝贵资产。您的组织拥有的一些最重要的资产是以信息的形式存在的，例如知识产权、战略计划和客户数据。保护这些信息对于您的组织继续运营、保持竞争力和满足监管要求至关重要。

## 介绍

---

AppScan on Cloud ( ASoC ) 是一种 SaaS 解决方案 (Software-as-a-service: 软件即服务)，可满足所有应用程序安全测试需求。它将Security的所有测试功能整合到一个服务中，为所有技术提供统一的体验。ASoC可以使用动态和静态技术扫描Web、移动和桌面应用程序。

- 动态分析 (DAST) 黑盒扫描

ASoC为生产、登台和开发环境的 Web 应用程序执行安全扫描。对于开发环境，它借助私有站点扫描技术来扫描开放 Internet 无法访问的应用程序。请参阅[动态 \(DAST\) 扫描](#)

- 静态分析 (SAST) 白盒扫描

ASoC对 Web 和桌面应用程序执行安全扫描。其静态分析包括智能发现分析 (IFA) 和智能代码分析 (ICA)。IFA 可以显著减少对安全发现进行分类的手动工作，使其仅关注积极的、高价值的问题。

ICA 有助于减少或完全避免其他技术所需的复杂配置，自动提高扫描精度。请参见[静态 \(SAST\) 扫描](#)

- 交互式分析 (IAST)

使用安装在应用程序上的代理，ASoC通过监控所有合法和恶意的交互，在运行期间识别应用程序中的安全漏洞。该过程是“被动的”，即 IAST 不发送自己的测试，因此可以无限期运行。请参阅[交互式 \(IAST\) 监控](#)

- 开源分析

ASoC识别应用程序中使用的开源软件包，报告具有已知漏洞的软件包，并提供补救建议。开源测试可以单独运行，也可以作为静态扫描的一部分运行。请参阅[开源测试](#)

ASoC具有启用其所有功能的 Web UI。但是，也可以使用 IDE 和自动化系统插件，因此如果不需要，则不需要与服务本身进行交互。例如，开发人员可以留在自己的集成开发环境 (IDE) 中，而无需在 IDE 和浏览器之间来回切换。IDE 插件还支持使用 Web UI 无法进行的代码交互。

为了补充其功能，ASoC还公开了一组全面的 REST API，用于驱动ASoC 中的操作。这使得ASoC非常适合集成到自动化环境中。客户可以使用 REST API 组成自己的工作流，而不是绑定到ASoC工作流。


ASoC有助于安全策略合规性。通过使用预定义的策略或定义自定义策略，可以轻松识别哪些应用程序不合规并需要注意。通过根据定义的策略进行过滤，可以确定问题修复的优先级。根据特定策略进行过滤有助于优先修复针对特定合规性的修复，而不是迷失在问题的海洋中。

ASoC还允许您运行个人扫描，它出现在应用程序的扫描列表中，但其扫描数据不会与应用程序的其余部分结果合并。这使开发人员能够运行扫描，而不会在整个应用程序数据中发现出现的问题。因此，在将代码推送到主代码流之前，可以检查个人扫描的结果是否存在关键问题。

ASoC有助于利用所有扫描功能来扫描多种类型的应用程序、管理整个组织的安全合规性以及自动化安全扫描操作。

## 注册及使用

---



创建账户

✓ 至少 8 个字符

✓ 至少 1 个数字

✓ 至少 1 个小写字母

First name \*

Last name \*

\* 表示必填字段

注册

返回登录





已发送验证电子邮件

要完成登录，请查看您的电子邮件。

返回登录



Hi YiZhang,


Welcome to HCL Software ID!

To verify your email address and activate your account,  
please click the following link:

Activate

This is an automatically generated message from [HCL Software](#). Replies are not monitored or answered.

## 申请免费试用

**AppScan**

# 免费试用 AppScan

我们的 AppScan 自助服务免费试用版为用户提供免费的 AppScan 实践体验。使用 HCL AppScan 的安全测试工具套件（包括用于 Web 和开源软件的 OSA、SAST 和 DAST）扫描应用程序中的 log4j CVE-2021-4041 漏洞。使用 AppScan 来：

- ◆ 持续监控应用程序的安全性
- ◆ 保持对监管要求的遵守
- ◆ 降低开源风险
- ◆ 利用完整的、可操作的报告

**立即开始您的 30 天免费试用！**

**注意：**试用版提供有限的 DAST 和 SAST 功能，但启用了用于 Log4j 漏洞扫描的完整开源分析 (OSA) 功能。

To get started, please [click here](#) to access our AppScan Trial Guide. Bookmark the page for easy reference.

Click OK to set up your HCL ID, which will be associated with the email you used to register.

**IMPORTANT NOTE:** You will automatically be redirected to a login page. You must click "Sign Up" at the bottom of the login window to start the setup process.

**Ok**

All the Best,  
HCL AppScan Team

点击 OK，跳转到试用界面



DAST

创建扫描



动态 (DAST)

扫描 Web 应用程序和 Web 服务。

or



动态：上传文件

从 AppScan Standard 文件扫描。



静态 (SAST)

扫描您的应用程序的源代码。



交互 (IAST)

在您的 Web 服务器上部署代理程序以持续监视您的应用程序。

扫描演示站点

创建扫描: 动态

URL 和域

登录

探索

网络

测试选项

Schedule

URL 和域 ?

从该 URL 启动扫描\*

https://demo.testfire.net?mode=demo

扫描演示站点

☐ 包含子域和平行域 (必须进行验证)

环境 ?

☒ 实时生产站点

在扫描期间，我们不会自动填写表单或执行 JavaScript 代码。扫描影响站点或扫描结构的可能性不大，但可能需要更长时间。

☐ 暂存或测试环境

在扫描期间，我们将自动填写表单并执行 JavaScript 代码，以尝试发现尽可能多的内容。这是更加全面的扫描，但也更可能影响站点的结构和稳定性。

< 上一步

取消

审查并扫描

# 创建扫描: 动态



## 摘要

### URL 和域

URL: **https://demo.testfire.net?m...**  
其他域: **无**  
环境: **生产**

### 登录

应用程序登录: **不需要**  
HTTP 认证: **不需要**

### 探索

探索: **自动探索**

### 网络

服务器位置: **公用网络**  
超时: **10 秒**

### 测试选项

## 首选项

扫描名称 \*

DAST 2021-12-18 https://demo.testfire.net?mode=der

- ☐ 作为个人扫描运行 ?
- ☐ 扫描完成时向我发送电子邮件

### 扫描启用 ?

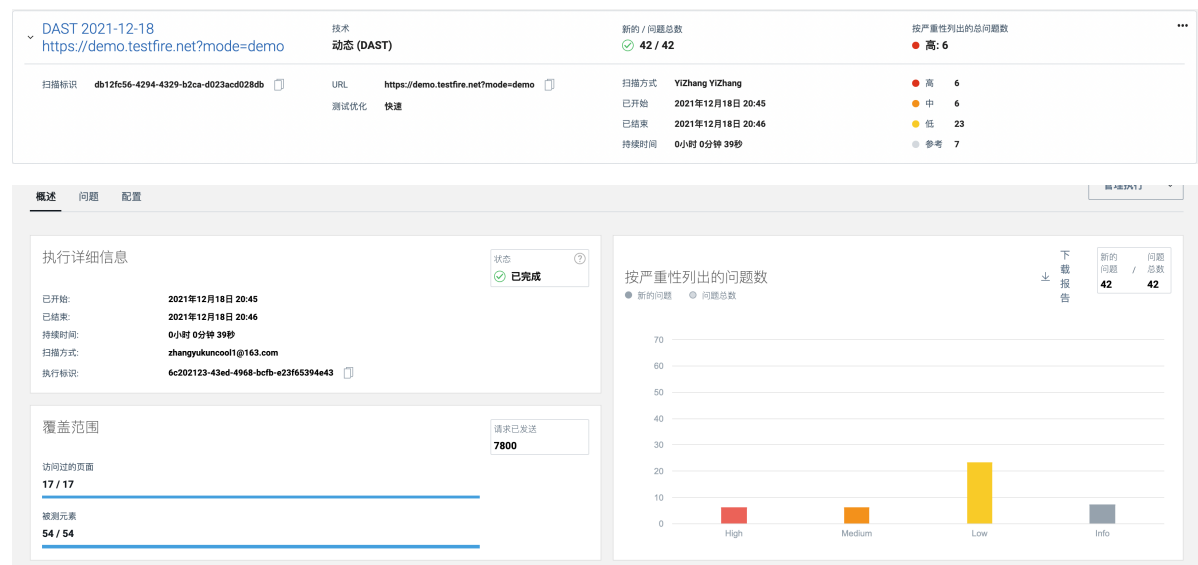
- ☒ 允许干预
- ☐ 包括发给扫描启用团队的消息

< 上一步

取消

立即扫描

## 扫描结果



概述	问题	配置	管理执行				
所有过滤器 (4)		快速过滤器: 严重程度: 极度严重、高度严重		不符合	清除过滤器		
项目总数: 42		编辑状态	安全报告	导出	列		
<input type="checkbox"/>	严重性	状态	问题类型	位置	首次发现	上次更新时间	调用方法
<input type="checkbox"/>	高	新建	反射型跨站点脚本攻击	Unavailable for free plan	2021年12月18日 20:46	2021年12月18日 20:46	Unavailable for free plan
<input type="checkbox"/>	高	新建	反射型跨站点脚本攻击	Unavailable for free plan	2021年12月18日 20:46	2021年12月18日 20:46	Unavailable for free plan
<input type="checkbox"/>	高	新建	反射型跨站点脚本攻击	Unavailable for free plan	2021年12月18日 20:46	2021年12月18日 20:46	Unavailable for free plan
<input type="checkbox"/>	高	新建	通过 URL 重定向钓鱼	Unavailable for free plan	2021年12月18日 20:46	2021年12月18日 20:46	Unavailable for free plan
<input type="checkbox"/>	高	新建	SQL 注入	Unavailable for free plan	2021年12月18日 20:46	2021年12月18日 20:46	Unavailable for free plan
<input type="checkbox"/>	高	新建	SQL 注入	Unavailable for free plan	2021年12月18日 20:46	2021年12月18日 20:46	Unavailable for free plan
<input type="checkbox"/>	中	新建	不充分帐户封锁	Unavailable for free plan	2021年12月18日 20:46	2021年12月18日 20:46	Unavailable for free plan
<input type="checkbox"/>	中	新建	链接注入 (便于跨站请求伪造)	Unavailable for free plan	2021年12月18日 20:46	2021年12月18日 20:46	Unavailable for free plan
<input type="checkbox"/>	中	新建	跨站点请求伪造	Unavailable for free plan	2021年12月18日 20:46	2021年12月18日 20:46	Unavailable for free plan
<input type="checkbox"/>	中	新建	通过框架钓鱼	Unavailable for free plan	2021年12月18日 20:46	2021年12月18日 20:46	Unavailable for free plan

## SAST

下载演示文件并上传

创建扫描: 静态

上载 IRX 文件

下载演示文件

上载完成

支持的文件类型: **IRX: Static Analyzer IRX 文件**

demo.irx 389 KB

如何生成 IRX 文件 ?

SAST Client Utility - CLI (Mac)

下载

下载并安装 AppScan Go! 或 SAST Client Utility CLI。这些工具可构建您的应用程序数据流表示形式并

上一步

取消

审查并扫描

摘要

上载 IRX 文件

文件名: demo.irx

首选项

扫描名称 \*

SAST 2021-12-18 demo.irx

☐ 作为个人扫描运行 ?

☐ 扫描完成时向我发送电子邮件

扫描启用 ?

☒ 允许干预

☐ 包括发给扫描启用团队的消息

< 上一步

取消

立即扫描

扫描结果

SAST 2021-12-18 demo.irx

静态 (SAST)

正在运行

扫描标识 7eb5bb44-dbeca-444d-bffc-b8a273b4270c

文件名 demo.irx

扫描方式 YiZhang YiZhang

已开始 2021年12月18日 20:54

已结束 -

持续时间 0小时 0分钟 2秒

高 -

中 -

低 -

参考 -

概述 问题 修复组 配置

管理执行

执行详细信息

状态 已完成

已开始: 2021年12月18日 20:54

已结束: 2021年12月18日 20:55

持续时间: 0小时 0分钟 28秒

扫描方式: zhangyukuncoo1@163.com

执行标识: ddb64c1e-3e55-4067-a3a9-f0d85a8b5ec0

扫描进度

0 %

语言

未找到语言

按严重性列出的问题数

新的问题 / 问题总数 81 / 81

下载报告

新的问题

问题总数

High 75

Medium 5

Low 1

Info 0



所有过滤器 (4)		快速过滤器: 严重程度: 极度严重、高度严重		不合规	清除过滤器		搜索
项目总数: 81		编辑状态	安全报告	导出		列	
<input type="checkbox"/> 严重性	状态	问题类型	位置	首次发现	上次更新时间	调用方法	
<input type="checkbox"/> 高	新建	Validation.Required	Unavailable for free plan	2021年12月18日 20:55	2021年12月18日 20:55	Unavailable for free plan	
<input type="checkbox"/> 高	新建	Validation.EncodingRequired	Unavailable for free plan	2021年12月18日 20:55	2021年12月18日 20:55	Unavailable for free plan	
<input type="checkbox"/> 高	新建	开源组件	Unavailable for free plan	2021年12月18日 20:55	2021年12月18日 20:55	Unavailable for free plan	
<input type="checkbox"/> 高	新建	SQL 注入	Unavailable for free plan	2021年12月18日 20:55	2021年12月18日 20:55	Unavailable for free plan	
<input type="checkbox"/> 高	新建	SQL 注入	Unavailable for free plan	2021年12月18日 20:55	2021年12月18日 20:55	Unavailable for free plan	
<input type="checkbox"/> 高	新建	SQL 注入	Unavailable for free plan	2021年12月18日 20:55	2021年12月18日 20:55	Unavailable for free plan	
<input type="checkbox"/> 高	新建	SQL 注入	Unavailable for free plan	2021年12月18日 20:55	2021年12月18日 20:55	Unavailable for free plan	
<input type="checkbox"/> 高	新建	反射型跨站点脚本攻击	Unavailable for free plan	2021年12月18日 20:55	2021年12月18日 20:55	Unavailable for free plan	
<input type="checkbox"/> 高	新建	SQL 注入	Unavailable for free plan	2021年12月18日 20:55	2021年12月18日 20:55	Unavailable for free plan	
<input type="checkbox"/> 高	新建	反射型跨站点脚本攻击	Unavailable for free plan	2021年12月18日 20:55	2021年12月18日 20:55	Unavailable for free plan	
<input type="checkbox"/> 高	新建	SQL 注入	Unavailable for free plan	2021年12月18日 20:55	2021年12月18日 20:55	Unavailable for free plan	
<input type="checkbox"/> 高	新建	反射型跨站点脚本攻击	Unavailable for free plan	2021年12月18日 20:55	2021年12月18日 20:55	Unavailable for free plan	

## 域验证

域验证

1 输入域

2 选择方法

3 验证

选择验证方法

您可以通过电子邮件或通过文件验证您的域

☒ 我会将验证文件添加到我的站点的根文件夹

根文件夹中存在该文件意味着向 ASoC 确认您有权扫描该站点。文件成功保存到域的根目录后，您便可以开始扫描。

☐ 向我发送包含验证链接的电子邮件

电子邮件包含可单击的链接，来确认您有权扫描该站点。只有在单击该链接后您才能够开始扫描。