Fortify SCA试用 华克斯

产品名称	Fortify SCA试用 华克斯
公司名称	苏州华克斯信息科技有限公司
价格	面议
规格参数	
公司地址	苏州工业园区新平街388号
联系电话	13862561363

产品详情

Fortify软件

强化静态代码分析器

使软件更快地生产

阅读强力手册

安全开发

开发人员编写代码时，尽可能早地确保修复。 DevInspect和静态代码分析器（在Premise）和Fortify on Demand将持续的安全测试和反馈直接传递给开发人员桌面。

安全测试

使静态和动态应用程序安全测试的自动化成为工作流程的一个自然部分。 软件安全中心和Fortify on Demand从一个界面提供企业级安全管理功能。

持续监控和保护

生产应用造成最da的威胁。 持续监控应用程序风险的变化，执行深度安全扫描，并与Fortify on Demand and Application Defender实时保护应用程序。

HI-RES-290926_1.jpg

HPE Security Fortify仍然是应用程序安全测试的领导者。

了解Gartner所说的话

Fortify软件

强化静态代码分析器

使软件更快地生产

“ 将FINDBUGS XML转换为HP FORTIFY SCA FPR | MAIN | CA特权身份管理员安全研究白皮书?

强化针对JSSE API的SCA自定义规则滥用

我们的贡献：强制性的SCA规则

为了检测上述不安全的用法，我们在HP Fortify
SCA的12个自定义规则中对以下检查进行了编码。这些规则确定了依赖于JSSE和Apache
HTTPClient的代码中的问题，因为它们是厚客户端和Android应用程序的广泛使用的库。

超许可主机名验证器：当代码声明一个HostnameVerifier时，该规则被触发，并且它总是返回"true"。

<谓词>

＜！[CDATA [

函数f：f.name是“ verify ”和f.enclosingClass.supers

包含[Class：name ==“ javax.net.ssl.HostnameVerifier ”]和

f.parameters [0] .type.name是“ java.lang.String ”和

f.parameters [1] .type.name是“ javax.net.ssl.SSLSession ”和

f.returnType.name是“ boolean ”， f包含

[ReturnStatement r：r.expression.constantValue matches “ true ”]

]]>

</谓词>

过度允许的信任管理器：当代码声明一个TrustManager并且它不会抛出一个CertificateException时触发该规则。抛出异常是API管理意外状况的方式。

<谓词>

＜！[CDATA [

函数f：f.name是“ checkServerTrusted ”和

f.parameters [0] .type.name是“ java.security.cert.X509Certificate ”

和f.parameters [1] .type.name是“ java.lang.String ”和

f.returnType.name是“ void ”而不是f包含[ThrowStatement t：

t.expression.type.definition.supers包含[Class：name ==

“ （javax.security.cert.CertificateException | java.security.cert.CertificateException） ”]

]]>

</谓词>

缺少主机名验证：当代码使用低级SSLSocket API并且未设置HostnameVerifier时，将触发该规则。

经常被误用：自定义HostnameVerifier：当代码使用高级HttpsURLConnection
API并且它设置自定义主机名验证器时，该规则被触发。

经常被误用：自定义SSLSocketFactory：当代码使用高级HttpsURLConnection
API并且它设置自定义SSLSocketFactory时，该规则被触发。

我们决定启动“ 经常被滥用 ”的规则，因为应用程序正在使用高级API，并且应该手动审查这些方法的重写。

规则包可在Github上获得。这些检查应始终在源代码分析期间执行，以确保代码不会引入不安全的SSL / TLS使用。

https://github.com/GDSSecurity/JSSE_Fortify_SCA_Rules

AuthorAndrea Scaduto |评论关闭|分享文章分享文章

标签TagCustom规则，CategoryApplication安全性中的TagSDL，CategoryCustom规则

Fortify软件

强化静态代码分析器

使软件更快地生产

HP Fortify静态代码分析器

Fortify SCA 5.0提供定制

为了帮助企业客户定制其应用程序安全规则和部署，Fortify已将规则开发和管理集成到Fortify SCA 5.0的审核工作台中，为开发人员通过管理安全开发的安全规则生成，编辑和排序提供了前所未有的灵活性。其中一些功能包括：

- 新的规则写入向导 - 用户可以快速创建自定义规则

回答一系列旨在确定代码中的问题的问题

这取决于唯yi的编码标准或专有库。

- API ScanView - Fortify SCA 5.0提供了一个用于呈现的界面

项目中使用的各种API，并突出显示未涵盖的API

通过Fortify安全编码规则包。从这个界面，Fortify SCA课程，用户可以

轻松创建相关API的新的自定义规则。

- Rulepack Manager - Fortify用于管理Rulepacks的界面

用户可以快速确定Rulepack的内容并允许它们

轻松过滤，排序和编辑规则。

- 规则编辑器 - 对于高级用户，Fortify的XML编辑器提供语法

突出显示，代码完成，验证和内联错误报告

适用于自定义规则。

Fortify SCA 5.0启用协作

全球企业需要跨开发团队的连接，能够在全球和全天候进行协作。 Fortify SCA 5.0为安全专业人员和应用程序开发人员提供了在不同视图中处理他们的项目的方法，允许两个组在不相互影响的情况下执行其功能。此外，此版本是第yi个应用程序安全解决方案，包括一系列跟踪和审核工具，可帮助开发人员在同一个项目上工作，而不管位置如何。最后，Fortify SCA 5.0集成了强大的报告功能，团队领导可以用来展示整个企业的其他利益相关者的进步。具体协作功能包括：

- 协作审核 - 团队成员现在可以发布一个

源代码扫描到基于Web的应用程序进行审查，评论

开启和分类问题。

- 开发者模式 - 以开发人员为中心的模式着重于众所周知

质量问题，如空指针解引用，内存泄漏和

更多 - 以非常低的假阳性率，精简安全

编码过程。开发人员可以专注于最重要的项目

他们，而安全专业人士可以看到所有潜在的问题

根据需要将他们带到开发商。

- 审计历史 - 在一个问题上执行的每个评论和行动

记录在时间轴上，以及时间戳和用户名

执行行动的人

- 手动审核整合 - 手动代码审查期间发现的问题

或其他形式的安全测试可以集成到审计

工作台。现在所有的代码级安全问题都可以合并在一个

强化SCA分析。

- 优先级排序 - 用户可以根据自己的需求分类问题

组织的命名，创建自定义问题文件夹和创建

过滤器自动填充文件夹中的特定类型的问题，

或者完全隐藏某些问题。

- 新的IDE支持 - Fortify SCA现在支持RSA 7，RAD 7和RAD 6。