源代码审计工具fortify sca 苏州华克斯信息

产品名称	源代码审计工具fortify sca 苏州华克斯信息
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

“ 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，fortify sca价格，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.ctantValue 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，源代码审计工具fortify sca价格，因为应用程序正在使用API，源代码检测工具fortify sca价格，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

FortifySCA与强化SSC之间的差异

Fortify SCA和Fortify SSC有什么区别？这些软件产生的报告是否有差异。我知道Fortify SSC是一个基于网络的应用程序。我可以使用Fortify SCA作为基于Web的应用程序吗？

Fortify SCA以前被称为源代码分析器（在fortify 360中），但现在是静态代码分析器。相同的首字母缩略词，相同的代码，只是名字改变了。

SSC（“软件安全中心”）以前称为Fortify 360 Server。惠普重新命名并进行了其他更改。

SCA是一个命令行程序。您通常使用SCA从静态代码分析角度扫描代码（通过sourceanalyzer或），生成FPR文件，然后使用Audit Workbench打开该文件，或将其上传到SSC，您可以在其中跟踪趋势。

审计工作台与SCA一起安装;它是一个图形应用程序，允许您查看扫描结果，添加审核数据，应用过滤器和运行简单报告。

另一方面，SSC是基于网络的;这是一个可以安装到tomcat或您喜欢的应用程序服务器的java。关于SSC的报告使用不同的技术，更适he运行集中度量。您可以报告特定扫描的结果，或历史记录（当前扫描与之前的扫描之间发生变化）。如果您想要扫描扫描的差异，趋势，历史等，请在上传FPR一段时间后使用SSC进行报告。

没有SSC，基本报告功能允许您将FPR文件（二进制）转换为xml，pdf或rtf，但只能给出特定扫描的结果，而不是历史记录（当前扫描和任何早期的）。

关闭主题：还有一个动态分析产品HP WebInspect。该产品还能够导出FPR文件，可以同样导入到SSC中进行报告。如果您希望定期安排动态扫描，WebInspect Enterprise可以做到这一点。

Fortify软件

强化静态代码分析器

使软件更快地生产

应用安全

HPE Security
Fortify提供端到端应用安全解决方案，具有灵活的测试内部部署和按需来覆盖整个软件开发生命周期。

跨SDLC的应用安全

到2020年，源代码扫描工具fortify sca价格，IT将需要每年发布120x应用程序。
随着发展速度的加快，满足这一需求，安全工作就要跟上。 无效安全测试效率低下且无效。
当这种方法与新SDLC的速度，集成和自动化相冲突时，安全性成为创新的障碍。
Fortify解决方案将应用程序安全性作为新的SDLC的自然部分，通过建立安全性实现上市时间。

源代码审计工具fortify sca价格-苏州华克斯信息由苏州华克斯信息科技有限公司提供。苏州华克斯信息科技有限公司是从事“Loadrunner,Fortify,源代码审计,源代码扫描”的企业，公司秉承“诚信经营，用心服务”的理念，为您提供更好的产品和服务。欢迎来电咨询！联系人：华克斯。