深度分析：Java的安全状况越来越糟 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/237/2021_2022__E6_B7_B1_E5_BA_A6_E5_88_86_E6_c104_237339.htm 在一年前的JavaOne大会上，Fortify Software创始人兼首席科学家Brian Chess作了一个标题为“ Java的12个技术陷阱及其应对方法 ”的演讲。一年过去了，我们为这些内在的脆弱性作了什么呢?这些弱点包括：XSS(跨站点的脚本)、SQL注射和允许引入C或者C 代码的本地方法——同它的BUG一起。如今，它可能会变得更糟，Chess说，他有证据证明这一点。Fortify——它的市场在于开源分析技术，已经涉及到了针对大型数据库的通用Java程序错误和弱点——不但来源于客户，而且来源于Java Open Review项目。在这个项目中，Fortify使用FindBugs——一个静态分析工具，能够在Java代码中寻找Bugs，能够审查开源项目代码，如：Apache、Azureus和Tomcat。它能够在线发布它发现的问题，然后把这些问题分享给那些特定代码脆弱性的维护人员。在这个项目中，Fortify所发现的开源系统代码缺陷密度是“ 天文数字 ”级别的。Chess指出，Fortify在去年的一个名为“ Net Trust ”的项目中所发现了大量错误——大约是每1000行代码有12215个错误。“ 这样的错误量显然是是过大了。 ”Chess说。更具有讽刺意义的是，Net Trust居然是Google用来为单点登陆和认证所建立的一个项目。“ 他们就像还是个没有做好作业的学生。 ”Chess说。Net Trust 只是能够证明Java安全陷阱的许多例证之一，虽然大家都对此有所了解，但是随着它应用的增长，还是会不断给那些使用它的程序员带来麻烦。当Java专家William Pugh意识到Java安全陷阱

变得更糟的时候，他完全同意Chess的意见。“ Xss变成了一个大问题。 ”他说。虽然像Fortify这样的工具集可以寻找XSS问题，但是它不能驱除你代码中所有的XSS漏洞。如果不包括所有的Web攻击，据统计，目前XSS漏洞正在变成最大的漏洞。Pugh是马里兰大学的计算机科教授，同时还是FingBug工具的作者，这个工具被用在Java开放检查项目中。举一个Sun说明书中的XSS漏洞的例子：try { firstname = request.getParameter("firstname"). } catch (Exception e) {e.printStackTrace(). }userName = firstname....pw.print(" Thanks for your feedback, " userName "!"). 这段代码允许黑客在应用程序中注入代码，它将在受害者的浏览器中运行。Chess说。“ 这段代码期望用户输入像Bob这样的名字 ”Chess在email中写道。“ 但是黑客能建立一个看起来像这样的数据：and then the victims browser would execute a function named sendDataToMotherShip()." ”安全的服务器端代码会判断它只包含特定的字符集并且不包含可执行脚本。为什么XSS会得到如此抨击?原因同10年前缓冲溢出的道理是一样的，这两个漏洞对黑客来说是十分重要的，因为这个漏洞允许黑客在系统中注入代码从而完全控制计算机。过去的棘手问题是缓存溢出，目前是XSS。“ 这两个漏洞的不同是，缓存溢出方法不太容易掌握，黑客需要对系统架构和本机上发生的各种情况十分精通。而XSS漏洞十分容易被利用——只要在当地的书店买本关于Java的书你就可以使用XSS了。 ”如果这些都来源于Sun，我们还能信任谁呢?事实是：查找最普遍的Java安全漏洞陷阱的责任应该完全由开发人员承担。这样情况就能够好转吗?也许会，但是也很困难，Chess说。一个解决方案是限制

浏览器执行XSS。这就需要更改Web标准同时使得浏览器变得更大。即使某些人说服了厂商来支持这个计划，它也需要把新的浏览器推广给数百万的用户。“ 我们转换到这上面的时间最少也得几年，基础架构和语言的变化需要很长的时间才能完成。 ” Chess说。“ 如果开发人员重视它的话，漏洞的数量会显著下降 ” Chess说。或许更有效的方法是同框架所有者和软件制造商来交流，从而使得Web成为安全的程序执行场所，Chess说。当然，这也不是能很快的解决。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com