

Fuzzingtool帮助OracleDBA删除SQL注入错误Oracle认证考试
PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/645/2021_2022_Fuzzingtoo_c102_645216.htm 数据库安全软件厂商Sentrigo Inc.发布了新的开源fuzzing工具FuzzOr，用于识别Oracle数据库软件应用中的漏洞。Sentrigo的创始人之一兼首席技术官Slavik Markovich说，有了FuzzOr，Sentrigo即将创建一款可以允许数据库管理员和程序员测试PL/SQL应用中的安全漏洞的工具。Markovich说，其它的漏洞评估工具有代表性的修复一系列错误，而FuzzOr是动态的，因为它没有于设置的清单。Markovich说：“(FuzzOr)式不同的，因为我认为没有其它可以做PL/SQL项目的工具了。FuzzOr扫描特殊的代码并分析(代码)寻找漏洞。” Fuzzing：SQL注入攻击新趋势警报研究人员：研究人员正在发现SQL注入攻击的新趋势，表明攻击者发现攻击新目标很容易。Fuzzing应该是安全软件开始程序的一部分吗？fuzzing是一种常见的软件测试方法，不能是你唯一的漏洞评估技术。Fuzzing可以有效地识别跨站脚本(XSS)漏洞吗？fuzzing可以找到软件中的漏洞，但是测试程序不能发现每个漏洞。Ed Skoudis解释了当查找跨站脚本漏洞的时候需要的其它工具。Oracle的安全专家，也是Oracle的安全网站PeteFinnigan.com的主管Pete Finnigan说FuzzOr是一款有用的工具，因为这是唯一免费分析PL/SQL中漏洞的实用工具。Finnigan说：“FuzzOr拥有优势，因为有了FuzzOr，就不需要查看软件代码再分析了，不然你就要分解它，使其做不同的事情。” Finnigan说，数据库管理员可能不能马上理解FuzzOr，但是它的使用相当简单，而且有简单的使用方法

。他说：“你可以在一个项目或者单独的一段代码上运行 FuzzOr，所以它的运行非常简单。(它)告诉用户哪些代码和参数容易受到工具，所以可以查看代码，并查找如何修复。

” Finnigan说，这个工具在检测与SQL注入和缓冲器负荷错误相关的漏洞方面也很理想，因为他们是使用PL/SQL编写的最常见的漏洞。Finnigan说，FuzzOr检测错误所用的时间是和它所运行的程序数量呈比例的，但是这种工具“相当快，不需要整晚都在运行。” Finnigan它不能在产品内部运行，因为工具的工能不只是读取。产品系统中使用的工具应该只能读取，防止不期望的变化，因此，这和FuzzOr是矛盾的。

Markovich说，这种工具不能修正问题，它只是告诉用户错误出在哪里。Markovich说，它并不作漏洞评估，检测或者加密。FuzzOr是免费的开源工具，也就是说许可证时GPL，而且只要用户拥有许可证，就允许用户改变或者增加代码。

Finnigan说所有的DBA都可以在内部尝试和使用的。Finnigan说：“FuzzOr是免费的，可扩展的，而且是用脚本语言编写的，软件代码是可以阅读的没有隐藏的东西，你可以看到它的工作方式。” 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