著名安全专家Litchfield对Oracle开火 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/167/2021_2022__E8_91_97_E5_90_8D_E5_AE_89_E5_c102_167100.htm 著名的袭虫猎人Litchfield为自己赋予的使命就是告诉全世界数据库软件并不安全特别是Oracle的数据库。Litchfield曾经公开批评Oracle，甚至要求Oracle首席安全官Mary Ann Davidson下台。Litchfield认为，长期以来，Oracle及其用户在安全领域里一直象鸵鸟一样把头插在沙子中。 Oracle采用了错误的方式来解决安全问题。 英国下一代安全软件的合作创办人Litchfield正在进行一场圣战。今年一月，他出版了一本Oracle黑客手册。手册的封面上说为读者提供了完整的访问和防护Oracle系统的方法。 在批判Oracle的同时，Litchfield却对微软极力推崇。他曾经公开声称微软最新的数据库软件SQL Server 2005是安全的。这种声明一定严重的伤害到了微软的主要竞争对手Oracle。Oracle已经眼看着一大块数据库市场划归了华盛顿Redmond的软件巨人。 在上周召开的Black Hat DC大会上，Litchfield讨论到了一种新的袭击技术使Oracle数据软件的漏洞问题更加严重。他向ZDNet澳洲的姐妹网站CNET News.com解释了揭露漏洞的必要性。 问：为什么您对数据库安全如此关注？还有其他那么多软件。 Litchfield: 数据库安全对于任何组织机构来说就象是王冠上的珠宝。这个星球上的每家机构都有数据库，而这组织机构存在的活力之源。没有什么比从源头进行把握更有效的安全措施。我们能够在周边进行安全工作，但是如果软件本身带有SQL injection这样的漏洞，那么安全措施就前功尽弃了。 我与Oracle的关系已经有所缓和。 尽管有防火

墙，尽管网络服务器已经被锁定，但是网络应用中的SQL injection缺陷就能让我们一路畅通的进入数据库服务器的后端。如果这个数据库没有采用最低权限，或者没有完全打好补丁，那么我们就能对数据库进行充分的访问并攫取全部数据。 数据库必须是安全的。问题是在最近以前，没有人真正的处理过数据库服务器的后端。也就是说过去人们采取的都不过是外围安全措施。 最近您对Oracle的数据库相当关注。是有什么特别的原因让您对Oracle倾注更多吗? Litchfield: 是的。SQL Server 2005是安全的。因为微软解决了问题。Oracle正在解决问题。对于IBM，我研究过DB2和Informix，并为他们指出了从缓存溢出到权限增加等大约50个bug，IBM安全部门的反应是成熟的。 最近，Oracle安全部门的反应就没那么成熟。他们气势汹汹的，与“ 这个家伙在让我们的产品更安全 ”的想法完全相反。不过他们的态度现在有所好转。Oracle正在开始理解我和他们站在同一条战线上，只是彼此的看法不同。 当Oracle这样的厂家态度强硬时，您就会变得更加强硬？ Litchfield: 是的。很遗憾我正是这样行事的。但是如果你不得不保护自己，那么就保护自己吧。我更愿意去工作，就象我对微软和IBM那样，与他们的安全响应团队一起工作。我们与微软和IBM拥有良好的关系。有什么比良好的关系好的成事方法呢？我可不想站在浑水中互相指责。 我与Oracle的关系有所缓解，他们理解这并不是一场意志上的对决。我努力使他们了解他们数据库所存在的问题，因为这些问题对我造成了直接的对影响。如果有人闯入数据库服务器然后窃取了我的信息，付出代价的是我，而不是Oracle/ 有人可能会认为这有点象敲诈。 Litchfield: 我可从来没有向Oracle索要过财

物。如果人们这么想，那么他们得到的信息可能有误。 那么微软也没有雇用你来说SQL Server 2005是安全的？ Litchfield: 我说微软的产品是安全的但是没有从微软那里得到什么报酬，如果任何人在SQL Server 2005中找到bug，那个人最好是我。如果别人找到什么bug,它会破坏我将来判断产品是否安全的能力。因此，如果在SQL Server 2005中的确存在bug，我希望是我首先发现。我很期待。 微软过去和现在是否是NGS软件的客户？ Litchfield: NGS的确在微软工作，但我们并不是受雇来说他们是安全的我们被雇来使他们的产品更安全。对于微软和NGS来说，现在以及将来的独立性都很重要。否则我们工作的正确性以及微软为使产品更安全所进行的努力就会遭到怀疑。这就是NGS 依然在为微软的产品提出安全建议的原因。 我听说您曾经担任SQL Server 2005的安全审计工作，是这样吗？ Litchfield: 我不能说具体的说到我们所做的项目。这样，如果有人对SQL Server是否比Oracle安全的问题存在疑问，他所要做的就是想想包括那么多顶级研究人员在内的很多人都曾经研究过两个产品，寻找过安全漏洞。而SQL Server已经很长时间没有被发现问题了。我再重复一遍，如果有人在SQL Server 2005中发现严重的漏洞，那么我希望那个人是我。 Oracle是否曾经是NGS软件的客户？ Litchfield: 是的，过去我们与Oracle合作过几个项目。 NGS软件的主要业务是什么? Litchfield:我们的业务分三个方面。我们销售评估安全状况和是否遵从萨班斯 - 奥克斯利法案的工具；我们为一些组织机构提供顾问服务；而且我们还进行漏洞调研并销售调研报告。 你们一般调研对象是什么样的机构？ Litchfield: 负责和保护关键性国家基础设施的政府机构。我们试着对他们的安全问

题提出事前警告。我们能够告诉他们某个产品存在缺陷，并且提供消除问题的策略。甚至没有厂家提供的补丁，系统也能得到保护。 靠无知来保证安全是行不通的，因为某个人的无知就是别人的生财之道。 NGS过去几年发展顺利，这些需求来自哪里？ Litchfield:主要是顾问工作。说起来惭愧，我最初要成立一家软件企业，但现在却更象一家顾问公司。尽管我没有放弃，但也算是我个人的一次失败。我们到某个阶段还会成为一家软件公司。 顾问一般怎么工作？ Litchfield: 他可能会做渗透测试，审查代码或者模仿入侵。我们所做的不是安装防火墙那样的工作，我们所从事的是高端工作。 是什么每天推动您进行工作？ Litchfield: 是因为我对次很擅长。如果你很擅长某件事情，您的动力就会更足。如果我是优秀的画家，我就会画很多作品。如果我对此一窍不通，我当然就不会费心劳力的去画画。我很享受我的工作。 是不是特别享受发现bug的工作？ Litchfield: 是的。这是一个关于分析的问题。如果我尝试推翻某个系统，我该怎么做呢？另一个原因是它会影响每个人的生活。现在，不是在拿死马当活马医。我知道明天数据库服务器将会更加安全。打个比方说，到那一天，更多的信用卡用户会更安全。 如果Oracle的人说你暴露缺陷的的行为实际上伤害了安全，你会怎么说？ Litchfield: 在他们假设的情况下这样做的确会提高了风险等级。好的，这的确是这类工作最主要的问题。不过，在风险度提高以后，人们会更倾向于保护自己的系统。 举例来说，我刚刚披露了一种能使没有特殊权限的入侵者利用只有具有更高权限用户才能使用的漏洞进行袭击的方法。现在我们知道这种担心是不对的，因为人们没道理知道这个缺陷以后不打补丁。 有人

在我贴出新方法后的零时间内利用我的方法修改入侵手段，并进行公布。于是任何人都可以使用这种手段，所以这的确增加了风险。 回头看2002年8月，我发布的一些代码被用做SQL Slammer病毒的基础。这属于最初的风险增加，但是短痛之后，打过补丁的SQL Servers数量增加了。短期风险成为了长期的受益。这是我对此的看法。 有人可能会说我们不想知道都有什么安全隐患，也就不会有人进行利用。你认为这有道理吗？ Litchfield: 我不这么认为。世界上总有坏人。如果没有好人来帮助厂家弥补这些漏洞，那么我们会自以为我们是安全的，但实际上我们并不安全。对安全问题视而不见是起不了作用的，因为一个人的无知就是另外一个人的生财之道。 什么使您觉得最烦恼？ Litchfield: 当人们说我增加了风险或者我的行为出于自私目的时，实际上并不是那样。不过我不会总那么受欢迎，我只是希望诽谤能够少一些。 您最近出版了Oracle黑客手册。您的目的是什么？ Litchfield: Oracle的安全世界里充斥着自鸣得意。我希望能够揭掉他们自我蒙蔽的毯子。外面有太多人认为Oracle的产品是安全的，他们无需采取任何措施。这是不负责任的，而我对此很在意。 你希望人们怎么看待你？ Litchfield: 我希望能够成为帮助人们认识到数据库安全的重要性的人。我希望能够通过我的工作，以及我对行业的了解来改造Oracle 和微软这样的企业处理安全问题的方式。 