黑客狙击Oracle系统的八大套路 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/493/2021_2022__E9_BB_91_E5_AE_A2_E7_8B_99_E5_c67_493541.htm Oracle的销售在向客户兜售其数据库系统一直把它吹捧为牢不可破的，耍嘴皮子容易，兑现起来可就不那么容易了。不管什么计算机系统，人们总能够找到攻击它的方法，Oracle也不例外。本文将和大家从黑客的角度讨论黑客是用哪些方法把黑手伸向了你原以为他们不能触及的数据，希望作为Oracle的数据库管理员能够清楚的阐明自己基础架构的哪些区域比较容易受到攻击。同时我们也会讨论保护系统防范攻击的方法。 1.SQL注入攻击 如今大部分的Oracle数据库都具有为某种类型网络应用服务的后端数据存储区，网页应用使数据库更容易成为我们的攻击目标体现在三个方面。其一，这些应用界面非常复杂，具有多个组成成分，使数据库管理员难以对它们进行彻底检查。其二，阻止程序员侵入的屏障很低，即便不是C语言的编程专家，也能够对一些页面进行攻击。下面我们会简单地解释为什么这对我们这么重要。第三个原因是优先级的问题。网页应用一直处于发展的模式，所以他们在不断变化，推陈出新。这样安全问题就不是一个必须优先考虑的问题。 SQL注入攻击是一种很简单的攻击，在页面表单里输入信息，悄悄地加入一些特殊代码，诱使应用程序在数据库里执行这些代码，并返回一些程序员没有料到的结果。例如，有一份用户登录表格，要求输入用户名和密码才能登录，在用户名这一栏，输入以下代码： cyw）；0select username， password from all_users；如果数据库程序员没有聪明到能够检查出类似的信

息并“ 清洗 ”掉我们的输入，该代码将在远程数据库系统执行，然后这些关于所有用户名和密码的敏感数据就会返回到我们的浏览器。 你可能会认为这是在危言耸听，不过还有更绝的。David Litchfield在他的著作《Oracle黑客手册》（Oracle Hackers Handbook）中把某种特殊的pl/sql注入攻击美其名曰：圣杯（holy grail），因为它曾通杀Oracle 8到Oracle10g的所有Oracle数据库版本。很想知道其作用原理吧。你可以利用一个被称为DBMS_EXPORT_EXTENSION的程序包，使用注入攻击获取执行一个异常处理程序的代码，该程序会赋予用户或所有相关用户数据库管理员的特权。 这就是Oracle发布的著名安全升级补丁Security Alert 68所针对的漏洞。不过据Litchfield称，这些漏洞是永远无法完全修补完毕的。 防范此类攻击的方法 总而言之，虽说没有万能的防弹衣，但鉴于这个问题涉及到所有面向网络的应用软件，还是要尽力防范。目前市面上有各式各样可加以利用的SQL注入检测技术。可以参照http://www.securityfocus.com/infocus/1704 系列文章的详细介绍。 还可以用不同的入侵检测工具在不同的水平上检测SQL注入攻击。访问专门从事Oracle安全性研究的Pete Finnigan的安全网站http://www.petefinnigan.com/orasec.htm，在该网页搜索“ sql injection ”，可以获得更多相关信息。Pete Finnigan曾在其博客上报告称Steven Feurstein目前正在编写一个称为SQL Guard 的pl/sql程序包，专门用来防止SQL注入攻击，详情请查看以下网页http://www.petefinnigan.com/weblog/archives/00001115.htm. 对于软件开发人员来说，很多软件包都能够帮助你“ 清洗 ”输入信息。如果你调用对从页面表单接受的每个值都调用清洗

例行程序进行处理，这样可以更加严密的保护你的系统。不过，最好使用SQL注入工具对软件进行测试和验证，以确保万无一失。 Oracle数据库是一个庞大的系统，提供了能够创建一切的模式。绝大部分的系统自带用户登录都配备了预设的默认密码。想知道数据库管理员工作是不是够勤奋？这里有一个方法可以找到答案。看看下面这些最常用的预设用户名和密码是不是能够登录到数据库吧： Username Password applsys apps ctxsys change_on_install dbsnmp dbsnmp outln outln owa owa perfstat perfstat scott tiger system change_on_install system manager sys change_on_install sys manager 就算数据库管理员已经很勤奋的把这些默认配对都改了，有时候想猜出登录密码也不是一件困难的事情，逐个试试“ oracle ”、“ oracle4 ”、“ oracle8i ”、“ oracle11g ”，看看碰巧是不是有一个能登录上去的。 Pete Finnigan提供了一份关于缺省用户和对应密码的名单，该名单非常全面而且是最新的，并包括已经加密的密码。如果你用all_users来进行查询，可以尝试并比较一下这份名单，详细名单请参阅：http://www.petefinnigan.com/default/default_password_list.htm. 防范此类攻击的方法 作为数据库管理员，应该定期审核所有的数据库密码，如果某些商业方面的阻力使你不能轻易更改容易被人猜出的密码，你可以尽量心平气和地和相关人员解释，用一些直观的例子来阐明如果不修改密码的话会有什么不好的事情发生，会有什么样的风险存在。 Oracle也提供了密码安全profile，你可以激活该profile，在某种水平上加强数据库密码的复杂性，还可以执行定期密码失效。要注意要把这个功能设置为只对通过网络服务器或中间层应用服务器登

录的事件起作用。 2. 蛮力攻击（Brute Force） 蛮力攻击，就像其名字所暗示的，就是不停的撬，直到“ 锁 ”打开为止的方法。对于Oracle数据库来说，就是用某种自动执行的进程，通过尝试所有的字母数字组合来破解用户名和密码。 Unix的管理员就可以利用一款名为John the Ripper的密码破解软件来执行这类的攻击。现在如果你下载某个补丁，你也可以利用这款软件来对Oracle进行蛮力攻击，敲开其密码。不过根据密码的复杂程度不同，这可能是个很费时的过程，如果你想加快这个进程，可以事先准备一张包含所有密码加密的表，这样的表叫做Rainbow table，你可以为每个用户名准备一张不同的rainbow table，因为这种密码加密算法把用户名作为助燃剂。在这里就不再深入介绍更多的细节问题了，大家可以查阅http://www.antsight.com/zsl/rainbowcrack/获得更多信息。 Oracle服务器的默认设置是，对某个特定帐户输错密码达十次就会自动锁定该帐户。不过通常“ sys as sysdba ”权限没有这个限制，这可能是因为如果你锁定了管理员，那所有人都将被锁定。这样的设置为我们黑客破解软件（OraBrute）如开辟了一条生路，它们会昼夜不停地敲打你数据库的前门，直到它乖乖打开为止。 防范此类攻击的方法 想要抵御此类攻击，可以使用之前提及的对付预设密码攻击的方法。不过好奇心过重的数据库管理员也可能下载上面提到的工具侵入自己的系统。这说明了你真正的风险来自何方。 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