快速通道

文档分类
- 红盟公告
- 新手上路
- 漏洞分析
- 工具介绍
- 安全配置
- 编程技术
- **安全技术** <=
- 业界动态

本类热门
- 如何利用黑客技术跟踪并分析一名目标人物
- 有关无线安全与黑客的话题
- 让我们回归(by 默难)
- 通用ShellCode深入剖析[转]
- Format String 漏洞介绍/总结(一)
- 结合实例解读ELF文件-阅读笔记(1)

Hackproofing Oracle Application Server

提交文章： wking
提交日期： 2004-02-17
文章属性： 翻译
文档类别： 安全技术
浏览次数： 今6次/总2365次

>>============A NGSSoftware Insight Security Research Publication============<<

Hackproofing Oracle Application Server
(A Guide to Securing Oracle 9)

>>============[straight translated by wking bblman@21cn.com 04.1] ============<<

Contents

Introduction
Oracle Architecture
Oracle Apache
-PL/SQL
-Buffer Overflows
-Directory Traversal
-Administration
-OWA_UTIL package
-PL/SQL Authentication By-pass
-PL/SQL Cross-site scripting
-OracleJSP
-Translation Files
-JSP SQL Poisoning
-Globals.jsa
-Physical Path mapping
-XSQL
-XSQLConfig.xml Access
-XSQL SQL Poisoning
-XSQL Style Sheets
-SOAP
-SOAP Application Deployment
-SOAP Configuration File
-SAMPLES
-Dangerous Samples
-DEFAULTS
-Dynamic Monitoring Services
-Perl Alias
TNS LISTENER
-Listener Security Issues
-EXTPROC and External Procedures
Oracle Database
-PL/SQL External Procedures
-Default User Logins and Passwords

Appendix A

Introduction(绪论)

恰恰与Oracle公司C.E.O：Larry Ellison所宣称的相反，Oracle 9存在漏洞。或许Oracle公司在其运营活动中标榜“ 神不可破 ”是为充分显示他们对更进一步生产安全产品所做出的承诺，但在实际中，Oracle公司的确十分注重其产品的安全性。Oracle公司的产品已经历并通过了14项独立的安全评估，其中包括Common Criteria assessment。在数据库领域这是相当了不起的成就，仅此Oracle公司就将其它的竞争对手远远甩在后面。目前Oracle 9正经历评估的考验。谨以此篇献给Oracle产品的用户，帮助他们对Oracle公司所承诺的安全环境有更深的了解。

要是某人为Oracle公司写一份安全方面的白皮书，他的功绩将与希腊君主科林斯王相姘美。Oracle公司开发了上百种产品，每件产品都应有其对应的专题说明。由于本文篇幅的限制，我们将讨论其中最普通的部分-从Oracle web前台到Oracle数据库服务器。主要的重点将放在Oracle web前台上，当然，我们还将简要了解数据库部分。对数据库部分的进一步研究将另外撰文探讨。经验表明，web服务器已无可厚非地成为攻击的第一个目标。本篇将演示攻击者是如何侵入基于Oracle的站点，获得web前台的操作权，直至最后控制数据库服务器。我们会讲解每种攻击方式，同时还会介绍其对应的防卫方法。针对本文一些问题的探讨你可以到http://metalink.oracle.com/发表，同时在那里你可以下载Oracle的安全补丁。

Oracle Architecture(Oracle体系结构)

典型的Oracle站点将由受防火墙保护Oracle web服务器和数据库服务器组成。Oracle web服务器将在由Oracle Application Server提供的高效环境下运行业主预先写好的应用程序。这些程序可以是PL/SQL 的应用程序、JSP、XSQL、java servlet或是基于SOAP的应用程序。(当然也可以是perl、fastcgi和其它被支持但又不是被经常使用的“ 非主流 ” 应用程序，故在此不作介绍。)在收到来自客户端的请求后，应用服务程序决定它是否有权限连接并访问后台数据库服务器的动态数据内容。

web服务器与数据库服务器之间的通讯是首先通过Listener构建的。Listener的职责是迅速建立连接到oracle数据库的工作，一旦联接建立，Listener便完成使命自动推出。但在接下来的讨论中我们将得知Listener的作用不止这个。Listener在执行数据库服务器扩展进程中还起一个关键的作用。

Oracle Web Front Ends(Oracle web前台)

Oracle公司曾出品他们自己的web服务器应用程序Oracle Web Listener但目前被广泛使用的是Apache。Oracle公司的Oracle Web Listener一直以来都被其存在的安全漏洞所困惑，但与Oracle应用程序服务器搭配的Apache服务器的情况也好不到哪里去。它易受多种如缓冲区溢出问题、拒绝服务攻击、众多危险样品页和apache缺省设置等的影响。每种应用环境都有各自的暴露系统的危险，但它们都是可以预防保护的。

PL/SQL

PL/SQL是Oracle公司针对结构队列语言SQL的程序语言扩展。PL/SQL插件包实质是存储在数据库上的程序。插件包中不仅有可被直接运行的程序，而且还存在有可以被其它插件包调用的内在功能函数。Apache的PL/SQL模式扩充web服务器的功能，使web网服器能够执行存储在数据库上的PL/SQL插件包。将PL/SQL模式比喻为使用存储化程序从外网进入Oracle数据库的一条通道一点都不为过。在缺省的情况下所有对web服务器的请求都被送到PL/SQL接受分配发送。客户端的URL请求将包含函数据库标识字符或者是DAD、数据库上PL/SQL插件的名称以及执行程序的名称。任何将被传递给程序的参数都将出现在如下的字符串中。
http://oracleserver/pls/bookstore/books.search?cname=War+and+Peace
上述的URL中有个称为“ bookstore ”的DAD，一个称为“ books ”的PL/SQL包，一个称为"search"的程序，它带有一个参数“ cname ”即被查找的书名。在wdbsvr.app文件中DAD描述了一节关于Apache是如何连接到数据库服务器的内容，当中还包含一些有关例如用户名和口令认证的细节。如果不能提供有效的凭证，请求将导致在web客户端提示，要求其出示访问许可。在与数据库服务器联接上后，数据库将装载books数据块并执行搜索同时返回搜索结果给web服务器，最后将结果传递给发送请求的客户端。

PL/SQL Buffer Overflows(PL/SQL缓冲区溢出)

PL/SQL模件存在有若干处缓冲区溢出漏洞。这些漏洞能被利用来在web服务器上运行恶意代码。在Windows NT/2000操作系统上apache进程的运行与本机SYSTEM相关，故任何代码都是在完整权限下执行。最初的漏洞可发生在一个获取系统管理员帮助页面的请求上。即便是系统管理员帮助页面已处于要求提供用户标识符或口令的保护下，帮助页面仍然不可靠。试试你的站点是否有如下漏洞：
http://oracleserver/pls/dadname/admin_/help/AAAAA.....

这里的AAAAAAA.....是一个超过1000的长字符串。如果apache进程违规存取或核心超负(瘫痪混乱)，服务器将易被攻击，应及时从Metalink安装补丁。如果补丁不起作用，你也可以试着将默认的管理员路径/admin_/更改为某些难被猜测或被强制破解的名字以减少被攻击的风险。你可以编辑在$ORACLE_HOME$\Apache\modplsql\cfg目录下的wdbsvr.app文件。

另一个溢出与前一个很相似，但这次没有dadname。
http://oracleserver/pls/admin_/help/AAAAA.....
这使得apache服务器以DAD的默认名将请求定向到/pls/dadname/admin_/help/AAAAA.....。在那里将发生缓冲区溢出。同样，该安装针对该地址的补丁并更改默认的管理员路径。

还有一种缓冲区溢出发生在当客户端使用“ 授权 ”的HTTP头发送凭证给web服务器。超长的口令也能引起溢出。而情况是基于64位骗码的恶意代码又很难被识别发现。

所有这些缓冲区溢出漏洞的补丁都可在Metalink站点下载并安装。

PL/SQL Directory Traversal(PL/SQL目录路径侵越)

PL/SQL模件可以被强制冲破其限定的web文件目录权限，而获得apache运行下的系统文件目录存取权限。试试你的站点是否有如下漏洞：
http://oracleserver/pls/dadname/admin_/help/..% 255Cplsql.conf
该问题的起因是由于PL/SQL模件进行的是二重URL译码，第一次将转换%255C为%5C，第二次又将%5C转换到“ \ ”。由此路径侵越成为可能。为避免此漏洞可从Metalink站点下载并安装对应补丁。

PL/SQL Administration(PL/SQL管理)

在缺省的状况下PL/SQL DADs管理员可远程控制而无须鉴别认证。这显然不是一件好事情。应该阻止攻击者试着使用缺省用户和口令，例如用SYS、SYSTEM或CTXSYS登入连接数据库服务器并通过运行命令行来更改用户名和口令以提升权限，直到最后控制服务器的机会。请求如下：
http://oracleserver/pls/dadname/admin_/
将显示出站点是否存在漏洞。如返回的是管理员页面，那么漏洞一定存在。要解决这个问题可按如下步骤操作。首先位于$ORACLE_HOME$\Apache\modplsql\cfg目录下的wdbsvr.app文件应被重新编辑。管理员路径应被改为某些难以被猜测或被强制破解的名字。同时还应加上口令。

PL/SQL Authorization Denial of Service(PL/SQL授权拒绝服务)

PL/SQL模件存在有拒绝服务漏洞。当模件收到一个晦涩的未被授权定义的客户端HTTP头例如Basic，Apache可能为此会违规存取或核心超负(瘫痪混乱)。应到Metalink站点安装由Oracle公司提供的补丁。

The OWA_UTIL PL/SQL Package(OWA_UTIL PL/SQL包裹)

OWA_UTIL包的存在与其它插件包一起提供了网络关联服务，如HTP：用于创造HTML内容，又如HTF：通过其函数产生HTML标注。这些都作为PL/SQL工具箱的一部分。

OWA_UTIL有许多程序可直接从网络调用，用以查看文件的标识signature、源代码showsource、内核脚本cellsprint、listprint和show_query_columns。

owa_util.signature

Signature仅简单地返回验证对owa_util存取的权限的消息。它不需要任何参数(尽管可以加，但不会起任何作用)
http://oracleserver/pls/dadname/owa_util.signature
如果返回的是这么一条消息：
This page was produced by the PL/SQL Cartridge on December 21, 2001 04:50 AM
那么可对owa_util进行操作。
如果未返回此消息而是代码500或403，那说明该文件可能已受保护。通常情况下取决于其被保护的程度，可试着加入空格、tab或回车键：
http://oracleserver/pls/dadname/%20owa_util.signature
http://oracleserver/pls/dadname/%0Aowa_util.signature
http://oracleserver/pls/dadname/%08owa_util.signature
当然一旦其它的程序能被调用，对其是否能获得存取权限也就变得毫无意义。

owa_util.showsource

调用Showsource能够返回插件的源编码。它需要一个参数，“ cname ”为其插件的名称。

http://oracleserver/pls/dadname/owa_util.showsource?cname=owa_util
这将返回owa_util插件的源编码。
http://oracleserver/pls/dadname/owa_util.showsoucre?cname=books

owa_util.cellsprint

Cellsprint允许执行任意SELECT SQL语句。它要求有一个参数“ p_theQuery ”，同时还可以加上“ p_max_rows ”参数来定义返回结果的条数。如果p_max_rows未被定义则默认为100行。
http://oracleserver/pls/dadname/owa_util.cellsprint?p_theQuery=select* from sys.dba_users
将在系统格式中返回100条dba_users表格的数据结果。
http://oracleserver/pls/dadname/owa_util.cellsprint?p_theQuery=select* from sys.dba_users&p_max_rows=1000
将从同一个表格返回1000行结果。
让我们特别关注一下sys.link$表。这个表的内容是连接服务器的数据库服务器列表名单。也有明文存储的连接时需要的用户名和口令列表文本。如果连接启动，它将成为第一台数据库服务器的代理。
http://oracleserver/pls/dadname/owa_util.cellsprint?p_theQuery=select* from sys.dba_users@other.world
这里用sys.link$代替Other.world将使得数据库服务器搜索出其它数据库主机列表，及它们连接时的用户名和口令当然还有有关sys.dba_users的内容。

owa_util.listprint

Listprint象cells print一样都可执行任意的SQL语句，不过它们有一处不同：当select*仅执行一列时，cells print无须改变仍有结果返回，而Listprint在写法上则需要用select a column来代替select *。
http://oracleserver/pls/dadname/owa_util.listprint?p_theQuery=select%20username%20from%20sys.dba_users&p_cname=&p_nsize=
这又产生一个无法回避的使用性问题，使用者又怎能知道服务器内表的字段名呢？

owa_util.show_query_columns

下例show_query_columns程序需要一个参数-“ ctable ”表的名字。
http://oracleserver/pls/dadname/owa_util.show_query_columns?ctable=sys.dba_users
该HTML页将返回表的字段名称列表。

可以预计当一个攻击者能存取OWA_UTIL插件时他们几乎便能得知数据库内的任何内容。因此必要的保护措施十分重要。OWA_UTIL只是你应该保护的一个例子。进一步地说所有dbms_*插件如htp包，utl* 包以及所有存在危险漏洞的部分都应受到保护。重新编辑wdbsvr.app文件并在增加一个排它的特权名单条目。

PL/SQL Authentication By-pass(PL/SQL认证迂回)

在特定情形下存取PL/SQL插件认证的进程可能被迂回绕过。想象一家允许顾客在线注册登记的联网银行系统。PL/SQL应用程序将负责有关匿名者注册和根据其数据库描述配置验证用户ID和口令的工作。一旦用户登记注册后他将能够存取访问实际的有着自身DAD的银行PL/SQL应用程序页面。该DAD是经过用户ID和口令验证通过的。尽管该用户的注册目的仅是试图获得权限以进入银行应用程序界面。打个比方，该银行站点的URLs如下所示：
http://oracleserver/pls/register/reg.signup
http://oracleserver/pls/banking/account.welcome
由于DADs只是简单地描述银行数据库应用程序的路径，故认证能被轻松地代替迂回，而只须直接输入：
http://oracleserver/pls/register/account.welcome
该问题存在的原因是由于在“ register ”DAD中配置的用户标识符和口令同样被允许访问数据库服务器。有2种方法保护这一缺陷。第一种银行应用程序应建立一个与用户注册数据库分开的不同的数据库。不对已获取登记注册的用户ID开放存取银行应用程序界面。另一个方法是编辑wdbsvr.app文件增加排它特许条目：“ exclusion_list ”。
exclusion_list= account*， sys*， dbms_*， owa*

PL/SQL Cross-site scripting vulnerabilities.(ByPL/SQL穿站脚本漏洞)

在默认的情况下对htp PL/SQL插件的存取是允许的。这些插件输出HTML和HTML标签。许多程序可被用于cross-site脚本攻击。
http://oracleserver/pls/dadname/htp.print?cbuf=<;script>alert(‘ Doh! ’)</script>
cross-site脚本攻击曾被广泛讨论，是种潜在威胁，故htp插件的使用应在wdbsvr.app文件中被否决。

OracleJSP

这个节将同时介绍JSP和SQLJSP的应用程序，他们都是由同一个OracleJSP组件分配的。

JSP Translation Files(JSP翻译文件)

当一网络客户端请求一个JSP页时该页自己需要被翻译成对应的java应用程序。这过程要求一个.java源文件编译成.class文件。这些文件是留在文件系统上并能通过网络执行。在缺省的情况下该项措施更本无法阻止匿名者存取包含有商业/应用逻辑的.java源文件甚至是存有用于连接数据库服务器的用户IDs和口令文件。后创造了3重转译文件。一个称作“ /foo.jsp ”的文件在接受请求时将生产下列转译文件：
_foo$jsp_StaticText.class
_foo.class
_foo.java
这些文件将被存储在“ /_pages ”的web目录下。如果foo.jsp位于某一子目录“ bar ”，例：“ /bar/foo.jsp ”，则一个命名为“ _bar ”的新子目录将和其它3份文件一起置于“ _pages ”目录下。想了解更多的有关命名标准的细节问题，请阅读：
http://download-west.oracle.com/otndoc/oracle9i/901_doc/java.901/a90208/trandepl.htm。
为防止攻击者对这些转译文件，有必要修正httpd.conf文件。得增加如下列条目：
<Location /_pages>
Order deny,allow
Deny from all
</Location>
注意,如果JSP页面是存储在一个别名目录(例：不是“ htdocs ”子目录)那就有必要增加条目：
<Location /dirname/_pages>
Order deny,allow
Deny from all
</Location>
这里的“ dirname ”是别名目录的名称。

JSP Global.jsa Access(JSP Global.jsa存取)

与JSP转译文件能被直接存取一样，JSP application's globals.jsa文件也能被直接存取。这些文件内含有应用扩充信息同时也经常包含用户IDs和口令。如果JSP应用程序使用的是globals.jsa文件，那么可在httpd.conf文件增加如下条目以加强保护，
<Files ~ "^\globals.jsa">
Order allow,deny
Deny from all
</Files>

JSP SQL Poisoning(JSP SQL中毒)

就象在其它所有的应用环境下一样，必须确保客户端输入的合法逻辑性。尤其是比如在客户端输入带单引号的SQL字符串时要确保引号成对匹配，在属性为数字的客户端输入的内容要确保是SQL语句数值。同时Oracle公司不支持像微软SQL服务器那样的可数SQL语句多层嵌套调用，Oracle在运用UNION或嵌套子SELECT语句上存在缺陷。

JSP Physical Path Mapping(JSP物理路径印射)

当请求一个不存在的JSP页时会出现java FileNotFoundException和一个包含真实文件物理路径信息的错误提示。为降低风险，对付此类问题可专门创建一张标准的JSP错误页来隐蔽信息。

XSQL

XSQL的配置文件可以在$/xsql/lib/XSQLConfig.xml下发现。这份配置文件包含例如数据库服务器主机名、用户标识符和口令等连接信息。由于这份文件能在虚拟目录下被找到故能经常被下载并浏览其内容。又假果这份文件已被保护并且任何对它的请求都会显示403禁止存取的回复，那仍然能通过使用如下XSQLServlet请求而获取该文件:
http://oracleserver/servlet/oracle.xml.xsql.XSQLServlet/xsql/lib/XSQLConfig.xml
路径迂回的方法攻克了对它的保护。

XSQL SQL Poisoning(XSQL SQL毒害)

基于一个经编辑的xsql文件可执行任何针对数据库服务器的SQL语句。分析如下代码:
<?xml version="1.0"?>
<xsql:query connection="demo" xmlns:xsql="urn:oracle-xsql">
SELECT * FROM USERS_TABLE WHERE NAME = '{@name}'
</xsql:query>
如果这被另存为file.xsql那这源码等同于：

http://oracleserver/file.xsql?name=foobar
并且结果将以XML形式返还浏览器。但通过在其后添加一单引号则可继续执行第二段语句：
http://oracleserver/file.xsql?name=foobar ’union select * from foo-
虽然前面已经说了，但仍有必要重申在用户端输入验证是否为合法SQL语句的重要性。能用来运行SQL语句的XSQL页应该被禁止。
http://oracleserver/xsql/java/xsql/demo/adhocsql/query.xsql?xml-stylesheet=none.xsl&sql=select+*+ from+sys.dba_users

XSQL Style Sheets(XSQL风格单)

早期版本的XSQL分析器对恶意XML程序攻击存在缺陷。通过特殊形式的表单可将存于远程站点web服务器的XML下载并执行。这个问题是被Georgi Guninski发现的。

SOAP(肥皂)

SOAP Application Deployment(肥皂应用程序的发展)

在Oracle 9iAS 版本1.0.2.2.1的标准安装中已默认加入了Oracle SOAP组件，并且允许远程匿名用户配置SOAP应用。这将很快引起广泛争论，并对该服务是否存在漏洞进行测试。
http://oracleserver/soap/servlet/soaprouter
是否服务器存在漏洞或应受保护。想了解更多信息请参见：
http://technet.oracle.com/deploy/security/pdf/ias_soap_alert.pdf

SOAP Configuration File(SOAP 配置文件)

应通过更改缺省值来保护soapConfig.xml文件。它既能被直接存取又能通过使用XSQLServlet被截取:
http://oracleserver/soapdocs/webapps/soap/WEB-INF/config/soapConfig.xml
http://oracleserver/servlet/oracle.xml.xsql.XSQLServlet/soapdocs/webapps/soap/WEB-INF/config/soapConfig.xml

DEFAULTS(缺省值)

与Oracle的Apache同时被安装的服务还有Dynamic Monitoring Services(动态监视服务)，它能被远程匿名登录。httpd.conf文件应被重新编辑以阻止对下列页面的存取。
Dynamic Monitoring Services
- http://oracleserver/dms0
- http://oracleserver/dms/DMSDump
- http://oracleserver/servlet/DMSDump
- http://oracleserver/servlet/Spy
- http://oracleserver/soap/servlet/Spy
- http://oracleserver/dms/AggreSpy

Oracle Java Process Manager
- http://oracleserver/oprocmgr-status
- http://oracleserver/oprocmgr-service (currently broken)

Perl Alias(Perl别名)

在某些版本的Oracle应用程序服务器上“ /perl ”虚拟的目录和“ /cgi-bin ”虚拟的目录被印射到同样的物理路径上。然而，“ /perl ”是被标记为一个与脚本别名相对应的apache别名。结果任何在“ /cgi-bin ”下的脚本源编码能通过“ /perl ”目录存取。这就应该更改httpd.conf文件，将/perl别名改为脚本别名。或者若暂不需要perl的情况下可安全剔除它。

SAMPLES(例子)

Dangerous Samples(危险的例子)

许多与Oracle应用程序服务器一起被安装了的例子若被滥用都将危及系统的安全性。例如：
http://oracleserver/demo/email/sendmail.jsp
能被用来发送恶意电子邮件。其它一些能于攻击SQL中毒漏洞，或是其它的一些漏洞，例如：
http://oracleserver/demo/basic/info/info.jsp
它将引起环境变量漏洞。其它还可能的是“ /cgi-bin/printenv ”、“ /fcgi-bin/echo ”、“ /fcgi-bin/echo2 ”。
在一台web服务器投入营运环境以前，所有的例子样品页和脚本都应被删除。

The TNS Listener(TNS监听器)

TNS，Transparent Network Substrate是Oracle顾客端通过Listener联接数据库的协议。Listener在TCP1521端口监听客户端对数据库的请求及接收那些等待连接并通知TCP端口上

监听器的Oracle进程的请求状态。后监听器通知该端口上的客户端，并直接与数据库进程连接。如果数据库被配置成多线程(MTS)服务器，那两个独立的进程将被创造，每位客户端都将各自接受固定端口上监听进程的服务。像与处理客户端连接请求一样，监听器在帮助数据库服务扩展程序上也起重要作用。先这么多，接下来将检验监听器自身。

Listener Security Issues(监听器安全问题)

先前版本监听器含有多重缓冲区溢出漏洞。这是被Covert Labs of Network Associates发现的，相关补丁可在Metalink站点得到。These aside out of the box,如过于轻心，即使是刚装了监听器仍将危及安全。也就是说，为应付攻击做一些修正很有必要。由于有关这些问题的文章甲骨文公司的霍华德·史密斯已在其它地方发表过，故在此就不重复了。

EXTPROC and External Procedures(EXTPROC和外部程序)

PL/SQL插件能被附加扩充调用应用于库或动态链接库的外部函数。当PL/SQL插件在数据库服务器执行时要求运行一个外部程序：oracle进程联接监听器并要求监听器载入相关的库，调用函数及其被附带传递过来的参数。监听器并没有装载库进入它自己的进程地址空间而是指导oracle连接到其它一个在Unix系统上被extproc的或Windows平台上extproc.exed的进程。Oracle强迫并连接到使用命名管道的extproc进程上并对监听器做了同样的请求。Extproc装载库并调用函数。在这个过程中没有提及任何权限认证。这开创一个耀眼并极端危险的安全漏洞。

攻击者很有可能会假装为一个Oracle进程，执行文件系统上任何DLL内的函数。是什么加剧了这个问题的严重性，是因为它能从远程在socket之上运行恶意程序。为此，攻击者能通过写一个在TCP上连接到监听器或extproc的exploit，而无须任何认证便能随心所欲地运行所有库函数。等到攻击者使用windows平台上的msvcrt.dll调用system()或通过unix平台上的libc调用exec()、system()时，世界就真的全完了。任何操作系统的命令行将以函数参数的形式被认为是oracle进程而得以光明正大地运行。在Unix系统上这将被认为是“ oracle ”帐户而在Windows NT/2000上这是缺省的本地系统帐户。这里我也不必再向大家介绍哪些是可能导致恐怖后果的系统命令行命令了吧。

几个方案可以用来帮助减轻此类攻击的风险。当然第一层的防护是使用防火墙。应禁止任何试图从1521端口获取监听。这不仅能帮助减轻此类问题的风险同时对其它问题也是一劳永逸的。倘若按照这样的描述文件设置web服务器那对源于web服务器发起攻击的风险将降到最小限度。进一步地还可从Metalink站点下载安装补丁。如果因某种原因未能安装补丁那就应对可以存取监听的机器进行限制。这就用到了基于IP地址的信任机制。该过程叫做“ valid node checking(有效节点检查) ”，这需要编辑在$ORACLE_HOME\network\admin目录下的sqlnet.ora文件，为其增加条目：
tcp.validnode_checking = YES
tcp.invited_nodes = (10.1.1.2, scylla)
方法便是用你所准许的主机地址代替10.1.1.2或scylla。那些未在括号中列出的其它任何非授权主机仍能基于TCP对监听器进行连接但监听器随后便将简单地停止连接，仅此而已。同时对应的授权节点应该经严格把关。另一个帮助减轻风险的方案是更改监听器默认的1521端口。虽然这不是一个伟大的解决办法，因为TCP端口扫描仪仍有很高的机率发现监听器，但该方法多少还起到点作用。最后，在Windows NT/2000系统上Oracle进程默认以本地SYSTEM的身份运行。建议为oracle进程建立一个新的低权限的帐号并为其赋予"Logon as a service"服务进程属性的权限。

Oracle Database Security(Oracle数据库安全)

就如文章开头所提到的那样，在数据库安全这块内容上我们将仅仅触及其中的一小部分。我们将在以后发表一份对其进行更详尽讨论的文章。这里我们将讨论2个方面：PL/SQL外部程序，用户登录和口令的缺省值。

PL/SQL External Procedures(PL/SQL外部程序)

前面我们刚讨论了通过隐瞒监听器在远程运行外部程序的漏洞，这里我们将检验数据库自身的外部程序漏洞。一个想要调用在oracle库内外部程序的帐号必须应具备CREATE LIBRARY权限。在默认的情况下以internal account、sys、system、ctxsys、mtxsys登录的都有此权限。尽管随后我们将专门讨论缺省内在登录帐目，但这里仍有必要再次强调更改默认口令的重要性。如果其中某些口令被攻击者利用，他将有权创建库以及那些看似和其它合法用户一样在正常运行的oracle进程，实质却是那些包含有能执行系统命令行命令的PL/SQL插件。一个典型的类似sql脚本如下：
Rem
Rem oracmd.sql
Rem
Rem Run system commands via Oracle database servers
Rem
Rem Bugs to david@ngssoftware.com
Rem

```
CREATE OR REPLACE LIBRARY exec_shell AS
'C:\winnt\system32\msvcrt.dll';
/
show errors
CREATE OR REPLACE PACKAGE oracmd IS
PROCEDURE exec (cmdstring IN CHAR);
end oracmd;
/
show errors
CREATE OR REPLACE PACKAGE BODY oracmd IS
PROCEDURE exec(cmdstring IN CHAR)
IS EXTERNAL
NAME "system" LIBRARY exec_shell
LANGUAGE C;
end oracmd;
/
show errors
```

运行如上脚本将生产下列结果：

```
C:\>sqlplus /nolog
SQL*Plus: Release 8.1.7.0.0 - Production on Thu Jun 7 14:25:38 2001
(c) Copyright 2000 Oracle Corporation. All rights reserved.
SQL> connect system/manager@orcl
Connected.
SQL> @c:\oracmd.sql
Library created.
No errors.
Package created.
No errors.
Package body created.
No errors.
SQL>
SQL> exec oracmd.exec ('dir > c:\oracle.txt);
```

在此需要大家引起警惕。为确保安全我们不得不对那些以有权建立库及插件的登录帐户进行行为监控。

Default User Logins and Passwords(用户登录和口令的缺省值)

Oracle的安装过程中，根据用户所选组件的情况会自动设定一定数量的默认帐户及口令。通常情况下口令与用户id是一样的，但也存在有不一样的情况。针对Oracle公司的第三方程序产品通常会设定一些弱口令。所有帐户都应及时更改缺省口令。又由于更换口令会影响到某些对应的功能性，故建议用户在操作前参照相关说明文档。在附录中列出了160条高频Oracle或第三方产品的默认口令及帐户。

Conclusion(结束语)

但愿本文对那些即将投入到互联网运营的Oracle服务器的安全设置起到一点帮助。在Oracle安装配置方面还有许多非常好的参考文献。
由O ’ Reilly出版的Oracle Security是一本极好的书。(http://oracle.oreilly.com)Pentest有限公司(http://www.pentest-limited.com)的Pete Finnigan在Oracle安全问题方面也有一些经典的文献。想要关注最新的有关oracle安全问题的资料请参见
http://technet.oracle.com/deploy/security/alerts.htm

NGSSoftware写了一个名叫OraScan的安全性评估扫描器用于审计Oracle web前台和Oracle应用程序。想要了解更多的有关内容请参见NGSSoftware站点，
http://www.ngssoftware.com/。

Appendix A – Default Oracle UserIDs and Passwords(附录 A)

SYS	CHANGE_ON_INSTALL
SYSTEM	MANAGER
AQJAVA	AQJAVA
AQ	AQ
CIDS	CIDS
SYMPA	SYMPA
LIBRARIAN	SHELVES
PANAMA	PANAMA
FROSTY	SNOWMAN
STARTER	STARTER
DES	DES
DBI	MUMBLEFRATZ
HLW	HLW
TRAVEL	TRAVEL

HCPARK HCPARK
ULTIMATE ULTIMATE
REP_MANAGER DEMO
REP_OWNER DEMO
OWA OWA
IMAGEUSER IMAGEUSER
MIGRATE MIGRATE
OPENSPIRIT OPENSPIRIT
ODS ODS
ODSCOMMON ODSCOMMON
OE OE
OLAPDBA OLAPDBA
OLAPSVR OLAPSVR
OLAPSYS OLAPSYS
ORACACHE ORACACHE
PM PM
PO7 PO7
PORTAL30 PORTAL30
PORTAL30_DEMO PORTAL30_DEMO
PORTAL30_PUBLIC PORTAL30_PUBLIC
PORTAL30_SSO PORTAL30_SSO
PORTAL30_SSO_PSPORTAL30_SSO_PS
PORTAL30_SSO_PUBLIC PORTAL30_SSO_PUBLIC
QS QS
QS_ADM QS_ADM
QS_CB QS_CB
QS_CBADM QS_CBADM
QS_CS QS_CS
QS_ES QS_ES
QS_OS QS_OS
QS_WS QS_WS
SH SH
UTLBSTATU UTLESTAT
VIRUSER VIRUSER
WKSYS WKSYS
USER1 USER1
USER2 USER2
USER3 USER3
USER4 USER4
USER5 USER5
USER6 USER6
USER8 USER8
USER9 USER9
USER USER
APPLSYSPUB PUB
SLIDE SLIDEPW
HR HR
JMUSER JMUSER
OWA_PUBLIC OWA_PUBLIC
CQSCHEMAUSER PASSWORD
WEBCAL01 WEBCAL01
CIS ZWERG
CISINFO ZWERG
MASTER PASSWORD
SYSADM SYSADM
ESTOREUSER ESTORE
SYSMAN OEM_TEMP
COMPIERE COMPIERE
OSP22 OSP22
PLSQL SUPERSECRET
PATROL PATROL
SITEMINDER SITEMINDER
REP_OWNER REP_OWNER
EJSADMIN EJSADMIN_PASSWORD
TURBINE TURBINE
ADMIN JETSPEED
OAS_PUBLIC OAS_PUBLIC
INTERNAL ORACLE
CTXSYS CTXSYS
MDSYS MDSYS
SCOTT TIGER
APPLSYS APPLSYS

APPS APPS
SAP SAPR3
ADAMS WOOD
AQDEMO AQDEMO
AQUSER AQUSER
BLAKE PAPER
CATALOG CATALOG
CDEMO82 CDEMO82
CDEMOCOR CDEMOCOR
CDEMOUCB CDEMOUCB
CDEMORID CDEMORID
CLARK CLOTH
COMPANY COMPANY
DBSNMP DBSNMP
DEMO DEMO
DEMO8 DEMO8
EMP EMP
EVENT EVENT
FINANCE FINANCE
FND FND
GPFD GPFD
GPLD GPLD
JONES STEEL
MFG MFG
MILLER MILLER
MMO2 MMO2
MODTEST YES
MOREAU MOREAU
NAMES NAMES
MTSSYS MTSSYS
OCITEST OCITEST
ORDPLUGINS ORDPLUGINS
ORDSYS ORDSYS
OUTLN OUTLN
PO PO
PO8 PO8
POWERCARTUSER POWERCARTUSER
BC4J BC4J
PRIMARY PRIMARY
PUBSUB PUBSUB
RE RE
RMAIL RMAIL
RMAN RMAN
MTS_USER MTS_PASSWORD
SAMPLE SAMPLE
!DEMO_USER !DEMO_USER
SECDEMO SECDEMO
TRACESVR TRACE
TESTPILOT TESTPILOT
TSDEV TSDEV
TSUSER TSUSER
VRR1 VRR1
MXAGENT MXAGENT
SDOS_ICSAP SDOS_ICSAP
TDOS_ICSAP TDOS_ICSAP
ORAREGSYS ORAREGSYS
CENTRA CENTRA
IMEDIA IMEDIA
OEMADM OEMADM
TAHITI TAHITI
CSMIG CSMIG
WEBDB WEBDB
WWW WWW
WWWUSER WWWUSER
WEBREAD WEBREAD
USER0 USER0
LBACSYS LBACSYS
ADLDEMO ADLDEMO
PERSTAT PERSTAT
REPADMIN REPADMIN
VIF_DEVELOPER VIF_DEV_PWD
VIDEOUSER VIDEOUSER

AUDIOUSER AUDIOUSER
AURORAORBUNAUTHENTICATED invalid
OSE$HTTP$ADMIN invalid
AURORAJISUTILITY$ invalid
XPRT XPRT
STRAT_USER STRAT_PASSWD

-Copyright (C) 2004 鲍博·朗曼公司 wking-

返回上页

Copyright © 2000-2004 **HUC** All Rights Reserved.
中国红客网络技术联盟 www.cnhonker.com
webmaster@cnhonker.net