2006年考试指导Oracle数据安全面面观(二) PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/142/2021_2022_2006_E5_B9_B4_E8_80_83_c102_142974.htm (二)来自内部的另外一个隐患--用户管理以及密码问题 在这里，其实作为一个差不多点的数据库管理员都很清楚，Oracle数据库本身就使用了很多种手段来加强数据库的安全性，经常见到的就有密码，角色，权限等等。那么我们就从最简单的DBSNMP说起： Oralce数据库如果采用典型安装后，自动创建了一个叫做DBSNMP的用户，该用户负责运行Oracle系统的智能代理（Intelligent Agent），该用户的缺省密码也是“ DBSNMP ”。如果忘记修改该用户的口令，任何人都可以通过该用户存取数据库系统。现在我们来看一下该用户具有哪些权限和角色，然后来分析一下该用户对数据库系统可能造成的损失。 启动SQL/PLUS程序，使用该用户登录进入： SQL> 0select * from session_privs. CREATE SESSION ALTER SESSION UNLIMITED TABLESPACE CREATE TABLE CREATE CLUSTER CREATE SYNONYM CREATE PUBLIC SYNONYM CREATE VIEW CREATE SEQUENCE CREATE DATABASE LINK CREATE PROCEDURE CREATE TRIGGER ANALYZE ANY CREATE TYPE CREATE OPERATOR CREATE INDEXTYPE 可以看到该用户不是SYS或SYSTEM管理用户，然而，它却具有两个系统级权限：UNLIMITED TABLESPACE和CREATE PUBLIC SYNONYM。 看到这两个权限你应该马上想到，这些都是安全隐患，尤其是UNLIMITED TABLESPACE，它是破坏数据库系统的攻击点之一。如果这时候你还依然认为，即使有人利

用这个没有修改的口令登录进数据库也造成不了什么损失的话，我就不得不提醒你：该用户具有UNLIMITED TABLESPACE的系统权限，它可以写一个小的脚本，然后恶意将系统用垃圾数据填满，这样数据库系统也就无法运行，并将直接导致最终的瘫痪。目前很多数据库系统都要求7X24的工作，如果出现了系统用垃圾数据填满的情况，那么，等数据库系统恢复时，恐怕不可挽回的损失已经造成了。