Oracle数据库安全性管理基本措施简介 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/221/2021_2022_Oracle_E6_95_B0_E6_c102_221985.htm 数据安全性是指保护数据以防止非法的使用，避免造成数据有意或无意的丢失、泄露或破坏。由于数据库系统中集中存放有大量的数据，这些数据又为众多用户所共享，所以安全约束是一个极为突出的问题。Oracle数据库系统在实现数据库安全性管理方面采取的基本措施有：◆通过验证用户名称和口令，防止非Oracle用户注册到Oracle数据库，对数据库进行非法存取操作。◆授予用户一定的权限，例如connect，resource等，限制用户操纵数据库的权力。◆授予用户对数据库实体(如表、表空间、过程等)的存取执行权限，阻止用户访问非授权数据。◆提供数据库实体存取审计机制，使数据库管理员可以监视数据库中数据的存取情况和系统资源的使用情况。◆采用视图机制，限制存取基表的行和列集合。在实际应用中，许多系统往往采用假用户(即非数据库用户)身份来管理，而真实用户的身份和登录口令就隐藏在应用系统中，或经过各种压缩加密等处理的配置文件中。但这样往往留下隐患，只要从分析应用程序入手，最终会分析出系统使用的数据库用户和口令，那么其安全性也就消失了。另一方面，系统代码是程序员写出来的，如果程序员有破坏意图，这种模式没有一丝的安全，因为他通过自己掌握的代码不经分析就轻而易举的获得登录用的数据库用户和口令。而采用真实数据库用户，存在着权限分配上的难度，特别是用户数和应用表数都很多时，这时必然要使用角色来管理应用权限的分配。当然不能直接将权限或

角色直接分配给用户，否则用户可以不同过应用系统，而采用SQL*PLUS等前端工具进入系统，进行一些没有经过应用系统检查的操作，产生的结果可能不符合应用逻辑。 我们在实践中发现，可以采用另一种方式利用角色功能，来防止上面出现的安全“ 漏洞 ”。在这种方式下，用户采用自己的标识和口令注册，但在未得到授权的角色前，是没有操纵数据库的任何权限。而授权用户使用的角色是埋在应用程序中的，只有应用程序才知道角色的名称和口令，从而激活角色，使用户拥有相应的权限。在应用系统之外，用户可以连接到Oracle，但没有激活相应的角色，他是不能做任何事情的，而开发人员不知道用户的标识和口令，他没有办法登录到Oracle，即使他能够推算出角色的标识和口令。 