

Oracle数据库数据安全面面观（一）（6）PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/143/2021_2022_Oracle_E6_95_B0_E6_c102_143100.htm 然后再利用触发

器when-new-from-instance执行callfrom或newform等命令，进入业务处理程序。这个主程序应当仅仅由管理员来掌握，编译之后将执行文件下发到各收费点的client端。在system用户下，利用oracle提供的pupbld.sql,建立表productuserprofile,执行下面这样的命令，限制在非开发状态sql命令的使用,例如 insert into productuserprofile(product,userid,attribute,charvalue) values(' sql*plus ' , ' test ' , ' connect ' , ' disabled ').insert into productuserprofile(product,userid,attribute,charvalue) values(' sql*plus ' , ' sfyy ' , ' 0delete ' , ' disabled ');这样，在sql状态下，根本无法连接到test用户，而在sfyy用户下，0delete命令将不能执行。当然，dba可以改变这些设置。当然了，这个仅仅是属于一种“应用技巧”，但是足可以把那些每天忙于更新系统的管理员舒服好几天了。但是另一方面，还要加强对源程序的管理，在client端只存放执行程序。加强审计，发现异常现象，及时处理。这样才可以做到更高一层的“安全”。在下面，我主要是向大家介绍一个rem对ghxxb制立数据库触发子,密码的加密程序。 rem 对ghxxb制立数据库触发子(当insert or 0update ghxxb时触发) 0drop trigger scjmmm. create or replace trigger scjmmm before insert or 0update of mm on ghxxb for each row begin :new.mm:=encrypt(:new.mm,:new.gh,to_char(sysdate, ' ss ')). end. / -----密码的加密程

```
序encrypt----- create or replace function encrypt
(inpass in varchar2,in_gh in varchar2,in_ss in varchar2) return
varchar2 is bcs varchar2(20). bcs1 number. cs number. jg number.
m_gh varchar2(4). m_mm varchar2(20). begin m_gh:=in_gh.
m_mm:=inpass. cs:=to_number(in_ss). if cs<13. jg:=jg*cs . end loop.
return(in_ss||substr(to_char(jg),1,14)). end. /总结上面的东西，
我们仅仅是从自身做起，知道了怎么维护oracle数据库安全这个
话题的“皮毛”。可是，对于这个似乎永远也说不完的话题，我们
光知道怎么从内部“防御”就够了吗？不要忘了，在外面，还有一
群虎视眈眈的“hacker”在盯着你的数据库--因为这里面有他们想
要的东西。 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
```