Oracle数据库密码破解易如反掌？ 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_143419.htm 这几天关于 Oracle 安全方面的消息很是令人震惊． 看来安全专家们是盯上了 Oracle. 随着对 Oracle 加密体系的研究不断深入，有人重新研究了 Oracle 的密码加密算法大致信息. 估计是为了引起 Oracle 技术圈子的注意，有好事者居然冒充 PSOUG 的 Daniel A. Morgan 在Google 新闻组贴出了这篇文章.这篇文章先从 Oracle 的密码设计目标开始("反向工程")，然后说了加密的大致思路是这样的： 用户名字和密码合并成一个字符串"s" "s" 转换为unicode 用 DES 的ncbc mode模式加密.Key为 0x123456789abcdef, 初始化向量为 0 同样的串用更新的初始化向量作为Key再次加密 更新的初始化向量作为 Hash 伴随着"潘多拉的盒子"被打开,很多密码 Crack 工具如雨后春笋般冒了出来，目前不下 10 多种．这其中比较引人注意的是 orabf 0.7 ,因为他是目前最快的工具．在 Pentium 4, 3 GHz (Windows XP) 的机器上每秒钟可以破解 1,100,000 个密码(感觉有些夸张). 著名的 Oracle 安全研究厂商 Red Database Security 也发布了自己的密码检查工具 Checkpwd ．这个工具和 orabf 一样，也是基于字典的．在该站点上还提供了一份各种 Oracle 密码破解工具的比较.非常值得一看！ 另外值得注意的是有人写出了针对 John the ripper 这个老牌破解工具的插件. 其实话说回来，这个关于 Oracle 密码加密的研究是早在 1993 年由 Bob Baldwin 发布的.不过当初似乎并没有引起人们注意．为什麼安全专家们开始翻老箱子底了呢? 一个原因是Oracle本身的安全问题的确不少，密码也的确存在不少问

题(比如，database link 的密码是明文保存在数据库里的)，另一个原因恐怕也和 Oracle 的首席安全官 Davidson 的大放厥词有关,恐怕是她的措辞大大激怒了安全专家们.好戏还有.....