数据安全之MySQL安全的二十三条军规 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/167/2021_2022__E6_95_B0_E6_8D_AE_E5_AE_89_E5_c103_167273.htm 使用MySQL，安全问题不能不注意。以下是MySQL提示的23个注意事项： 1.如果客户端和服务器端的连接需要跨越并通过不可信任的网络，那么就需要使用SSH隧道来加密该连接的通信。 2.用set password语句来修改用户的密码，三个步骤，先“ mysql -u root ”登陆数据库系统，然后“ mysql> 0update mysql.user set password=password(newpwd) ”，最后执行“ flush privileges ”就可以了。 3.需要提防的攻击有，防偷听、篡改、回放、拒绝服务等，不涉及可用性和容错方面。对所有的连接、查询、其他操作使用基于ACL即访问控制列表的安全措施来完成。也有一些对SSL连接的支持。 4.除了root用户外的其他任何用户不允许访问mysql主数据库中的user表； 加密后存放在user表中的加密后的用户密码一旦泄露，其他人可以随意用该用户名/密码相应的数据库； 5.用grant和revoke语句来进行用户访问控制的工作； 6.不使用明文密码，而是使用md5()和sha1()等单向的哈系函数来设置密码； 7.不选用字典中的字来做密码； 8.采用防火墙来去掉50%的外部危险，让数据库系统躲在防火墙后面工作，或放置在DMZ区域中； 9.从因特网上用nmap来扫描3306端口，也可用telnet server_host 3306的方法测试，不能允许从非信任网络中访问数据库服务器的3306号TCP端口，因此需要在防火墙或路由器上做设定； 10.为了防止被恶意传入非法参数，例如where ID=234，别人却输入where ID=234 OR 1=1导致全部显示，所以在web的表单中使

用或""来用字符串，在动态URL中加入"代表双引号、#代表井号、代表单引号；传递未检查过的值给mysql数据库是非常危险的； 11.在传递数据给mysql时检查一下大小； 12.应用程序需要连接到数据库应该使用一般的用户帐号，只开放少数必要的权限给该用户； 13.在各编程接口(C C PHP Perl Java JDBC等)中使用特定‘ 逃脱字符 ’函数； 在因特网上使用mysql数据库时一定少用传输明文的数据，而用SSL和SSH的加密方式数据来传输； 14.学会使用tcpdump和strings工具来查看传输数据的安全性，例如tcpdump -l -i eth0 -w -src or dst port 3306 | strings。以普通用户来启动mysql数据库服务； 15.不使用到表的联结符号，选用的参数 --skip-symbolic-links； 16.确信在mysql目录中只有启动数据库服务的用户才可以对文件有读和写的权限； 17.不许将process或super权限付给非管理用户，该mysqladmin processlist可以列举出当前执行的查询文本；super权限可用于切断客户端连接、改变服务器运行参数状态、控制拷贝复制数据库的服务器； 18.file权限不付给管理员以外的用户，防止出现load data /etc/passwd到表中再用0select显示出来的问题； 19.如果不相信DNS服务公司的服务，可以在主机名称允许表中只设置IP数字地址； 20.使用max_user_connections变量来使mysqld服务进程，对一个指定帐户限定连接数； 21.grant语句也支持资源控制选项； 22.启动mysqld服务进程的安全选项开关，--local-infile=0或1 若是0则客户端程序就无法使用local load data了，赋权的一个例子grant insert(user) on mysql.user to user_name@host_name.若使用--skip-grant-tables系统将对任何用户的访问不做任何访问控制，但可以用mysqladmin flush-privileges或mysqladmin reload来

开启访问控制；默认情况是show databases语句对所有用户开放，可以用--skip-show-databases来关闭掉。 23.碰到Error 1045(28000) Access Denied for user root@localhost (Using password:NO)错误时，你需要重新设置密码，具体方法是：先用--skip-grant-tables参数启动mysqld，然后执行mysql -u root mysql,mysql>0update user set password=password(newpassword) where user=root.mysql>Flush privileges.，最后重新启动mysql就可以了。 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