SQL注入漏洞入侵的过程及其防范措施 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/139/2021_2022_SQL_E6_B3_A8_E5_85_A5_E6_c100_139653.htm ASP编程门槛很低，新手很容易上路。在一段不长的时间里，新手往往就已经能够编出看来比较完美的动态网站，在功能上，老手能做到的，新手也能够做到。那么新手与老手就没区别了吗？这里面区别可就大了，只不过外行人很难一眼就看出来罢了。在界面的友好性、运行性能以及网站的安全性方面是新手与老手之间区别的三个集中点。而在安全性方面，新手最容易忽略的问题就是SQL注入漏洞的问题。用NBSI 2.0对网上的一些ASP网站稍加扫描，就能发现许多ASP网站存在SQL注入漏洞，教育网里高校内部机构的一些网站这种漏洞就更普遍了，可能这是因为这些网站大都是一些学生做的缘故吧，虽然个个都很聪明，可是毕竟没有经验，而且处于学习中，难免漏洞多多了。本文主要讲讲SQL注入的防范措施，而要明白这些防范措施的用处，须先详细讲解利用SQL注入漏洞入侵的过程。新手们看明白啦。 相当大一部分程序员在编写代码的时候，没有对用户输入数据的合法性进行判断，使应用程序存在安全隐患。如这是一个正常的网址http://localhost/lawjia/show.asp?ID=444，将这个网址提交到服务器后，服务器将进行类似Select * from 表名 where 字段="&amp.ID的查询(ID即客户端提交的参数，本例是即444)，再将查询结果返回给客户端，如果这里客户端故意提交这么一个网址:http://localhost/lawjia/show.asp?ID=444 and user>0，这时，服务器运行Select * from 表名 where 字段=444 and user>0

这样的查询，当然，这个语句是运行不下去的，肯定出错，错误信息如下： 错误类型： Microsoft OLE DB Provider for ODBC Drivers (0x80040E07) [Microsoft][ODBC SQL Server Driver] [SQL Server]将 nvarchar 值 ’sonybb’ 转换为数据类型为 int 的列时发生语法错误。 /lawjia/show.asp, 第 47 行 但是别有用心的人从这个出错信息中，可以获得以下信息：该站使用MS__SQL数据库，用ODBC连接，连接帐号名为：sonybb。所谓SQL注入（SQL Injection），就是利用程序员对用户输入数据的合法性检测不严或不检测的特点，故意从客户端提交特殊的代码，从而收集程序及服务器的信息，从而获取想得到的资料。通常别有用心者的目标是获取网站管理员的帐号和密码。比如当某个人知道网站管理员帐号存在表login中，管理员帐号名为admin，他想知道管理员密码，这里他从客户端接着提交这样一个网址
：http://localhost/lawjia/show.asp?ID=444 and (Select password from login where user_name= ’admin’)>0，返回的出错信息如下： 错误类型： Microsoft OLE DB Provider for ODBC Drivers (0x80040E07) [Microsoft][ODBC SQL Server Driver] [SQL Server]将 varchar 值 ’ ！@＃＊&admin’ 转换为数据类型为 int 的列时发生语法错误。 /lawjia/show.asp, 第 47 行 你知道吗？上面标红的部分就是管理员帐号admin的密码！虽然很复杂，让人看几遍也记不住的，但它就这样显示在你面前了，这时您就可以用这个帐号和密码接管人家的网站了！这时你可能还会说，如果他不是事先知道管理员帐号存在表login中，而且知道管理员帐号为admin，那他就不可能获得管理员密码。你错了，只要人家愿意多花时间尝试，他将可以获得数据

库连接帐号权限内所能获得的所有信息！具体过程请参看网上的这篇文章：SQL注入漏洞全接触。 当然这个过程是很烦琐的而且要花费很多的时间，如果只能以这种手动方式进行SQL注入入侵的话，那么许多存在SQL注入漏洞的ASP网站会安全很多了，不是漏洞不存在了，而是利用这个漏洞入侵的成本太高了。但是如果利用专门的黑客工具来入侵的话，那情况就大大不同了。手动方式进行SQL注入入侵至少需要半天或一天乃至很多天的时间，而利用专门的工具来入侵就只需要几分钟时间了（视网速快慢决定），再利用获得的管理帐号和密码，上传一个从网上下载的ASP后门程序，就轻易获得整个网站的管理权限了，甚至整个服务器的管理权限。最有名的一种SQL注入入侵工具是NBSI 2.0，现在已经出到2.0版本了，不过，人家正式名称不叫SQL注入入侵工具，而叫做网站安全漏洞检测工具。有了这个所谓的检测工具，使得入侵存在SQL注入漏洞的ASP网站成了小儿科的游戏，那些既不懂ASP又不懂SQL、年纪小小的男性青年常常得以在一天之内入侵十多个ASP网站，他们以此获得内心的极大满足。他们似乎也非常讲究职业道德，往往并不破坏网站数据和系统，常见的破坏方式大都仅仅是改换掉网站的主页，留下"善意的警告"，如：你的网站存在SQL注入漏洞，请管理员做好防范措施！并声明"我没有破坏数据和系统"，有的还要借机发布一下他的倡导："国内网站大家不要入侵"，最后，签上他的鼎鼎大名是必不可少的程序。 如此大的成就多数情况下仅需动动鼠标就做到了。打开最新版的NBSI 2.0，输入地址到A区，注意网址必须是带传递参数的那种，点击右边的检测按钮，即出来B区信息，显示当前用户为sonybb的权限

为PUBLIC，当前库为lawjia。有点可惜啊，如果是SA权限的话，就可以跨库注入了。不过，这个权限也足够获取该网站管理员帐号和密码了。点C区下的自动猜解按钮，即出来当前库lawjia中的各种表，哇，login表中一定是存管理员帐号和密码的吧？选中它吧，接着点击D区下的自动猜解按钮，立即出来login表里的列名称，果然是存放用户名和密码的啊，太棒了！赶快打上勾，迫不急待的点击E区下的自动猜解按钮。激动人心的时刻就要到来啦，只见唰唰地几下，帐号与密码全部出来了。剩下的事就是辨别哪一个帐号是管理员了。