SQL注入

1.简介

SQL注入（Structured Query Language Injection）技术在国外最早出现在1999年，我国在2002年后开始大量出现，

SQL注入攻击是存在于常见的多连接的应用程序中的一种漏洞，攻击者通过在应用程序预先定义好的查询语句结尾加上额外的SQL语句元素，欺骗数据库服务器执行非授权的任意查询。这类应用程序一般是Web应用程序，它允许用户输入查询条件，并将查询条件嵌入SQL语句中，提交到数据库中执行。通过构造畸形SQL语句攻击者能够获取额外的信息数据。

当应用程序使用输入内容来构造动态SQL语句以访问数据库时，会发生SQL注入攻击。如果代码使用存储过程，而这些存储过程作为包含未筛选的用户输入的字符串来传递，也会发生SQL注入。SQL注入可能导致攻击者使用应用程序登陆在数据库中执行命令。如果应用程序使用特权过高的帐户连接到数据库，这种问题会变得很严重。在某些表单中，用户输入的内容直接用来构造动态SQL命令，或者作为存储过程 的输入参数，这些表单特别容易受到SQL注入的攻击。而许多网站程序在编写时，没有对用户输入的合法性进行判断或者程序中本身的变量处理不当，使应用程序 存在安全隐患。这样，用户就可以提交一段数据库查询的代码，根据程序返回的结果，获得一些敏感的信息或者控制整个服务器，于是SQL注入就发生了。

SQL注入是从正常的WWW端口访问，而且表面看起来跟一般的Web页面访问没什么区别，所以目前市面的防火墙都不会对SQL注入发出警报，如果管理员没查看IIS日志的习惯，可能被入侵很长时间都不会发觉。但是，SQL注入的手法相当灵活，在注入的时候会碰到很多意外的情况，需要构造巧妙的SQL语句，从而成功获取想要的数据。

2.SQL注入的主要危害

（1）、未经授权状况下操作数据库中的数据，比如管理员密码，用户密码等信息；

（2）、恶意篡改网页内容，宣传虚假信息等；

（3）、私自添加系统帐号或者是数据库使用者帐号；

（4）、网页挂广告、木马病毒等；

（5）、上传webshell，进一步得到系统权限，控制电脑.获得肉鸡。

3.SQL注入攻击过程

（1）、SQL注入一般存在于形如：http://xxx.xxx.xxx/abc.asp?p=YY的网站中。

（2）、在http://xxx.xxx.xxx/abc.asp?p=YY 后面追加“and 1=1”，并访问该网址即http://xxx.xxx.xxx/abc.asp?p=YY and 1=1 应该与访问原地址得到的结果相同。

（3）、在http://xxx.xxx.xxx/abc.asp?p=YY 后面追加“and 1=2”，并访问该网址即http://xxx.xxx.xxx/abc.asp?p=YY and 1=2应该与访问原地址得到的结果不同，并提示数据库错误。

（2，3同时满足则此网站必定存在SQL漏洞，可以进行sql注入攻击。）

（4）、访问http://xxx.xxx.xxx/abc.asp?p=YY and exists (select \* from 网站数据库常用表段名)

网站数据库常用表段名：admin users administrator 等，如果进入的网页像是正常网页，证明存在该表段名。进而寻找网站的管理员名、密码等信息。

（5）、访问http://xxx.xxx.xxx/abc.asp?p=YY and exists (select [网站数据库常用字段名] from 第4步找到的可入侵表名)

网站数据库常用字段名：admin password username 等，如果进入的网页是正常网页，证明存在该字段名。进而寻找网站的管理员名、密码等信息。

（6）、访问http://xxx.xxx.xxx/abc.asp?p=YY and exists (select \*from第4步找到的可入侵表名where第5步找到的可入侵字段名like '\_ ‘)

（7）、访问http://xxx.xxx.xxx/可入侵后门字段名，找到网站后门。

（8）、利用从数据库中查到的敏感数据进入网站后门。

1. SQL注入攻击的防范

（1）程序员加强自身技术水平，使用固定开发的标准；

（2）在提交服务端处理之前对数据的合法性进行检查；

（3）封装客户端提交信息；

（4）替换或删除敏感字符、字符串；

（5）错误信息不返回给用户；

（6）数据敏感信息非常规加密，防止信息外泄。

（7）加强数据库检查（表结构是否出现异常、是否有多余数据等）、IIS日志检查（SQL注入攻击往往会大量访问某一个存在漏洞的网页，日志文件会急剧增加，通过查看日志文件的大小以及日志文件中的内容。）；

（8）不用字串连接建立SQL查询，而使用SQL变量，因为变量不是可以执行的脚本；

（9）使用SQL注入防范系统。